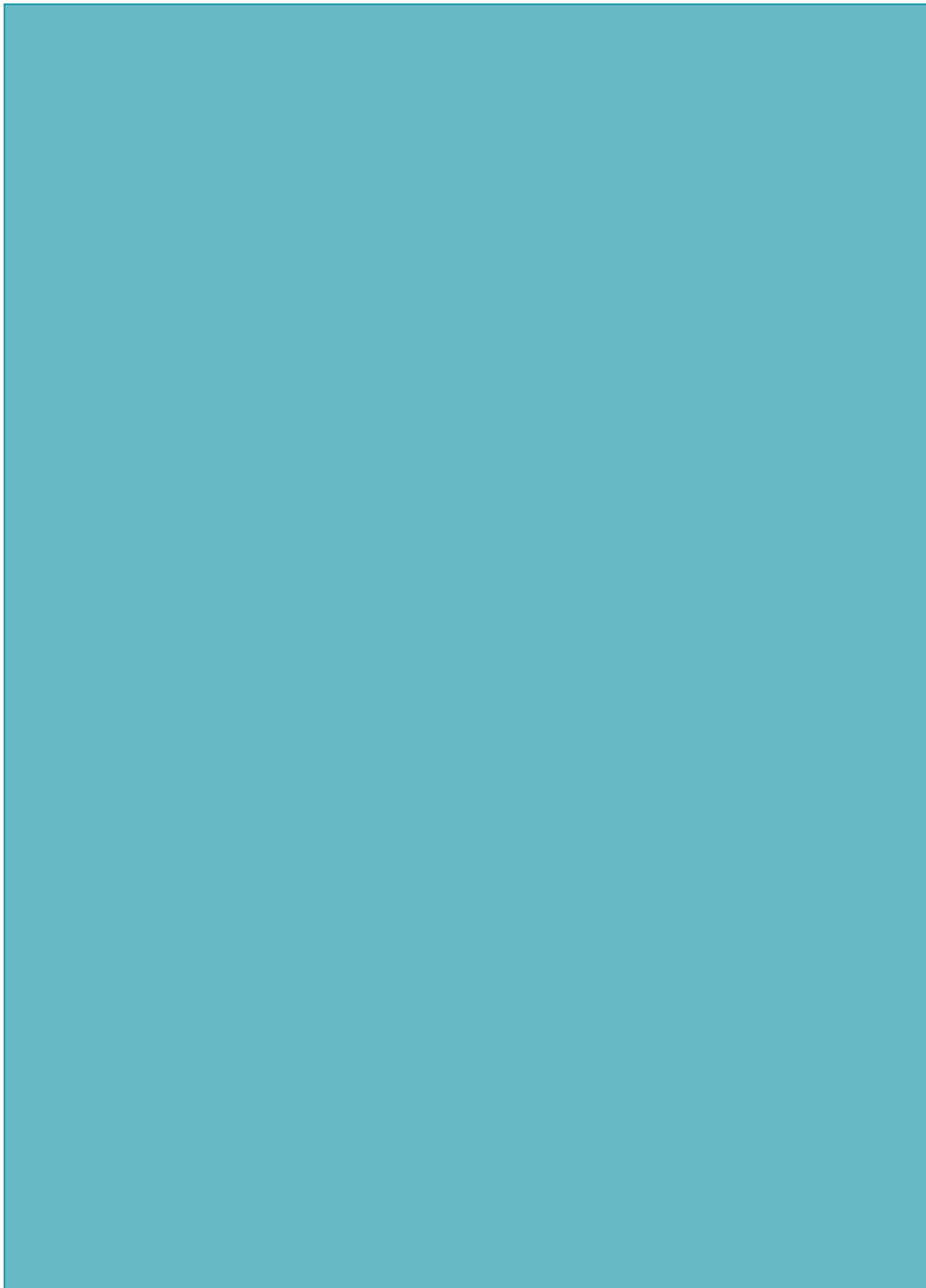


Intelligence Requirements and Threat Assessment

10



CHAPTER TEN



Intelligence Requirements and Threat Assessment

Information is needed to make decisions – the higher the quality and the more comprehensive the information, the more sound the decision. If an executive is going to make a decision about implementing a new program, he or she needs information on the costs, benefits, and risks of the program as well as the more difficult dimension of what benefits will be lost if a program is not implemented. Typically, the information sought is not conclusive, but based on probability, the experience of others, experimentation, logic or, sometimes, an educated guess. Not having sufficient reliable information makes the decision process more difficult (and risky).

The same phenomenon applies to the operational world of criminal intelligence. To adequately assess the threats from a terrorist group or criminal enterprise, information is needed for a comprehensive analysis. Oftentimes during the course of the analytic process, critical information is missing that prevents a complete and accurate assessment of the issue. This is a gap, an unanswered question related to a criminal or terrorist threat. An intelligence requirement is identified and information needs to aid in answering questions related to criminal or terrorist threats.¹⁷⁷

In order to adequately ASSESS THE THREATS from a
TERRORIST GROUP or CRIMINAL ENTERPRISE, information
is needed for a COMPREHENSIVE analysis.

Filling Gaps/Fulfilling Requirements

¹⁷⁷ FBI Office of Intelligence. *The FBI Intelligence Cycle: Answering the Questions....* A desk reference guide for law enforcement. (Pamphlet form). (July 2004).

The information collection process needs to be focused so that specific information needs are fulfilled. This increases efficiency of the process and ensures that the right information needs are being targeted. Too often in the past a “dragnet” approach was used for collecting information, and analysts and investigators would examine the information in hopes of discovering the “pearls” that may emerge. As illustrated in Figure 10-1, there are a number of differences between the traditional approach and the requirements-based approach to information collection. In essence, the requirements-based approach is more scientific; hence, more objective, more efficacious, and less problematic on matters related to civil rights.

Figure 10-1: Traditional Collection vs. Requirements-Based Collection¹⁷⁷

Tradition-Based	Requirements-Based
• Data-driven	• Analysis-driven
• Exploratory	• Contemplative
• Emphasizes amassing data	• Emphasizes analysis of data
• Infers crimes from suspected persons	• Infers criminal suspects from crimes
• An aggregate approach to information collection (dragnet); even mere suspicion	• Targeting/specificity on information regarding reasonable suspicion of crimes
• Explores all general inferences about potential criminality	• Selectively explores crime leads based on priorities and evidence
• Explores collected information to see if there are questions to answers	• Answers questions by collecting and analyzing information
• Develops intelligence files for contingency needs, (i.e., just in case information is needed)	• Develops intelligence files in support of active crimes and investigations
• Statistics produced for descriptive purposes	• Statistics produced for decision making

Since this is a scientific process, the intelligence function can use a qualitative protocol to collect the information that is needed to fulfill requirements. This protocol is an overlay for the complete information collection processes of the intelligence cycle. The numbered steps in the box below are action items in the protocol, the bulleted points are illustrations. This is not a template, but a process that each agency needs to develop to meet its unique characteristics.

1. Understand your intelligence goal
 - Arrest terrorists and/or criminals
 - Prevent or mitigate terrorists attacks
 - Stop a criminal enterprise from operating
2. Build an analytic strategy
 - What types of information are needed?
 - How can the necessary information be collected?
3. Define the social network
 - Who is in the social circle of the target(s)?
 - Who is in the regular business circle of the target(s)?
 - Who has access to the target(s) for information and observation
 - What hobbies, likes, or characteristics of the target's social behavior are opportunities for information collection, infiltration, and observation?

¹⁷⁷ Carter, David L. (2003). *Law Enforcement Intelligence Operations*. Tallahassee, FL: SM&C Sciences, Inc.

4. Define logical networks
 - How does the enterprise operate?
 - Funding sources
 - Communications sources
 - Logistics and supply
5. Define physical networks
 - Homes
 - Offices
 - Storage and staging areas
4. Task the collection process
 - Determine the best methods of getting the information (surveillance, informants, wiretaps, etc.)
 - Get the information

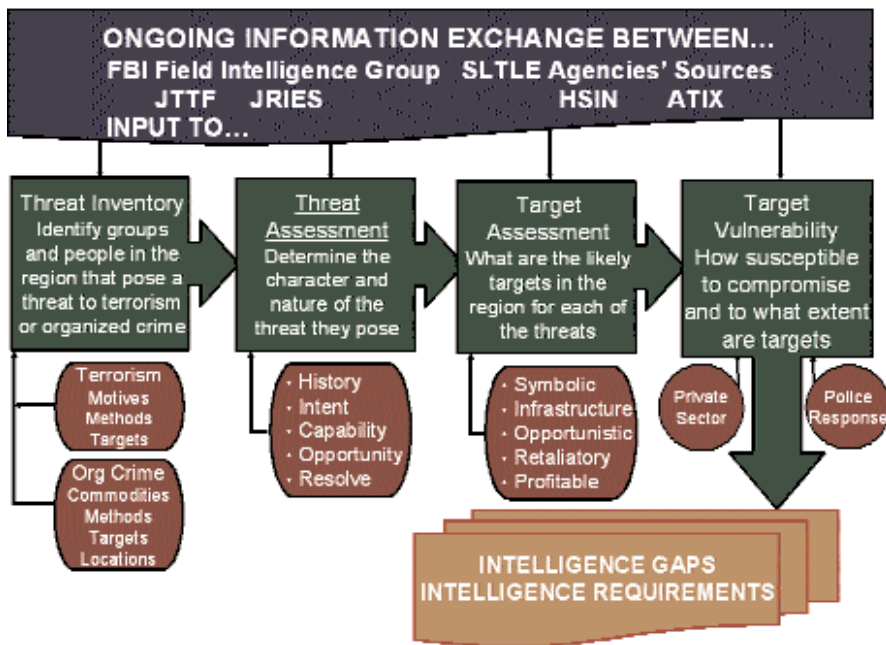
As information sharing becomes more standardized and law enforcement intelligence as a discipline becomes more professional, law enforcement agencies at all levels of government will use the requirements-driven process. In all likelihood, this approach will become a required element for information sharing, particularly with the FBI and the Department of Homeland Security (DHS).

Threat Assessments

Threat assessments are often discussed, but the process remains elusive to many state, local, and tribal law enforcement (SLTLE) agencies (Figure 10-2). There are four key variables in the process:

1. Threat Inventory.
2. Threat Assessment.
3. Target Assessment.
4. Target Vulnerability.

Figure 10-2: Threat Assessment Model for SLTLE¹⁷⁸



Threat inventory: The threat inventory requires the law enforcement agency to identify groups and individuals within the agency's region¹⁷⁹ that would pose possible threats. These may be international terrorists, domestic extremists, individuals who have an extreme special interest ideology, or a criminal enterprise. The type of information sought centers on identifying answers to certain questions: Who are the people involved? What is their group affiliation, if any, and what do they believe? To understand extremists it also is useful to identify their motives, methods, and targets. With criminal enterprises, the variables are methods, commodities, and locations. In either case, understanding how the criminal entity operates and what it seeks to accomplish can provide significant insight into their ability to act. Care must be taken to collect and retain the information in a manner that is consistent with 28 CFR Part 23 guidelines.

Threat assessment: Each threat identified in the inventory must be assessed with respect to the level of the threat posed. Some individuals make threats, but do not pose a threat. Conversely, some individuals and groups pose threats without ever making a threat. To fully assess their

178 This model was prepared by David L. Carter, Michigan State University, as part of a training program on Intelligence Requirements and Threat Assessment for the Bureau of Justice Assistance (BJA)-funded State and Local Anti-Terrorism Training (SLATT) program.

179 Realistically, the threat assessment must be done on a regional, rather than jurisdictional, basis because a specific threat and/or target will likely have an impact on the jurisdiction.

threat capacity, several factors need to be examined: What is the history of the groups? Have they committed attacks or crimes in the past? If so, what was the modus operandi (MO) and character of the act? Does the group have the capability to actually commit terrorist acts or crimes? If so, how robust is that capability? Are unique opportunities present for the group to commit an act? What appears to be the resolve or the commitment of the group? Factors such as these can develop an image to aid in determining the character of the threat posed by individuals and groups in the inventory.

Target assessment: In light of the nature of the groups in the threat inventory, probable targets can be identified in the region. It is rare that a specific target can be identified, but based on history, statements, threats, and the nature of an extremist group's ideology, the array of targets can be narrowed. Similarly, criminal enterprises tend to have targeted commodities that they traffic or types of frauds they perpetrate.

Target vulnerability: The last variable is to assess each of these targets to determine how vulnerable they are to attack. This often involves working with the private sector and often crime-prevention specialists within the law enforcement agency. Given the difficulty of identifying specific targets, the goal is to ensure that each potential target in the region is hardened against an attack.

When information is not available about the factors in this assessment model, there is an intelligence gap that must be filled by a requirement.

FBI Intelligence Requirements Templates

When going through this threat assessment process, the SLTLE agency will need information from the FBI to aid in fully identifying and assessing threats. As noted by the FBI:

State and local agencies or entities are served by the FBI and have specific needs for tailored intelligence. ... To appropriately address the information needs of state and local agencies, certain procedures can enhance this process. These include:

- Identifying, prioritizing, and addressing state and local information needs.
- Sharing intelligence, analytical techniques, and tools.
- Timely distribution of appropriate intelligence.
- Seek feedback from state and local [law enforcement concerning the] effectiveness of the support.¹⁸⁰

To facilitate this information exchange, the FBI Office of Intelligence developed a template (Figure 10-3) expressly for SLTLE agencies to use for logging Intelligence Information Needs (IINs) or intelligence gaps they identify. IINs are questions expressed by customers of the FBI and other intelligence producers, the answers to which support law enforcement functions. IINs are not operational leads or questions on the status of investigations or operations. Intelligence gaps are unanswered questions about a criminal, cyber, or national security issue or threat. To illustrate this further, the FBI developed a sample of “baseline” IINs (Figure 10-4). The SLTLE agency should coordinate its use of IINs and information exchange with the Field Intelligence Group (FIG) of the FBI Field Office servicing it.

180 FBI Office of Intelligence. (2003). *FBI Intelligence Production and Use. Concept of Operations Report.* (unpublished report). Washington, DC: FBI Headquarters Divisions and the Office of Intelligence, p. 18.

IN ORDER TO FACILITATE THIS INFORMATION EXCHANGE, the FBI Office of Intelligence has developed a template expressly for SLTLE agencies to be used to log Intelligence Information Needs or intelligence gaps they identify.

CONCLUSION

The intent of intelligence requirements and threat assessments is to provide a comprehensive, consistent model for managing the threats to a community. These processes are not necessarily easy; however, the outcomes they provide can be priceless.



Figure 10-3: Intelligence Information Needs (IINs)

Purpose: This form should be used to log IINs or intelligence gaps identified by state, local, or tribal law enforcement agencies in your area of responsibility. IINs are questions expressed by customers of the FBI and other intelligence producers, the answers to which support law enforcement functions. IINs are not operational leads or questions on the status of investigations or operations. Intelligence gaps are unanswered questions about a criminal, cyber, or national security issue or threat.

<u>IIN</u>	<u>Requesting Organization</u> (Agency, department, organization)	<u>Dissemination Instructions</u> (Customer name, position title, mailing address, contact number, LEO or other official e-mail address)



Figure 10-4: “Baseline” Intelligence Information Needs (IINs)

Purpose: This template provides a list of sample IINs that can be presented to state, local, and tribal law enforcement partners as a baseline from which to review intelligence gaps, select issues relevant to their investigative needs, and identify additional intelligence and collection requirements.

<u>IIN</u>	<u>Requesting Organization</u> (Agency, department, organization)	<u>Dissemination Instructions</u>
<p>National and local threat assessment reports.</p> <ul style="list-style-type: none"> - Reliability of the information received - Group planning attack(s) - Target(s) - Why is the target a target? - Suspected method of attack - Weapons of attack - Time frame of attack - Response of federal entities <p>Global, national and local trend reports regarding organizations and structures of active terrorist, criminal, drug, and hate groups in the US.</p> <ul style="list-style-type: none"> - Identity of suspects and their roles in the local area - Territorial reach - Decision-making processes; degree of subordinate autonomy - Command-control-communications techniques, equipment, network <p>Global, national and local trend reports regarding capabilities, intentions, MO of suspect groups in the US</p> <ul style="list-style-type: none"> - Types of weapons, explosives, or WMD - Methods of moving, storing and concealing weapons, contraband and human traffic - Special/technical expertise possessed by groups 		<p>(Customer name, position title, mailing address, contact number, LEO or other official e-mail address)</p>

<u>IIN</u>	<u>Requesting Organization</u>	<u>Dissemination Instructions</u>
<p>Illegal activities of suspect groups in local jurisdictions</p> <ul style="list-style-type: none"> - illegal production/acquisition of CBRNE materials/precursors, illegal drugs or substances, prohibited items or persons - illegal arms trade, theft, diversion, sales; smuggling of aliens, terrorists, or prohibited items; human trafficking - HAZMAT dumping; environmental crimes; trafficking in endangered species - links between criminal groups and terrorist or foreign intelligence organizations; bribery/extortion/corruption of public officials <p>Identity, roles of US and foreign players sponsoring/supporting criminal, terrorist, espionage activities in local jurisdictions</p> <ul style="list-style-type: none"> - criminal function of each operative or entity; extraterritorial reach - associated commercial/charitable entities; front/cover organizations - chain of custody in transport of critical technology, illegal items/persons - overseas connections (official, unofficial, private sources); group sympathizers - financial dependencies; extent of group's reliance on external support, funds <p>Intelligence/security activities of suspect groups</p> <ul style="list-style-type: none"> - surveillance, reconnaissance, concealment, "cover" activities; safe houses - counterintelligence and physical security techniques and tactics - COMSEC operations; ability to monitor LEC communications - informant/mole network available to suspect groups - production of, access to false/counterfeit documents and identification - deception, disinformation operations and techniques 		

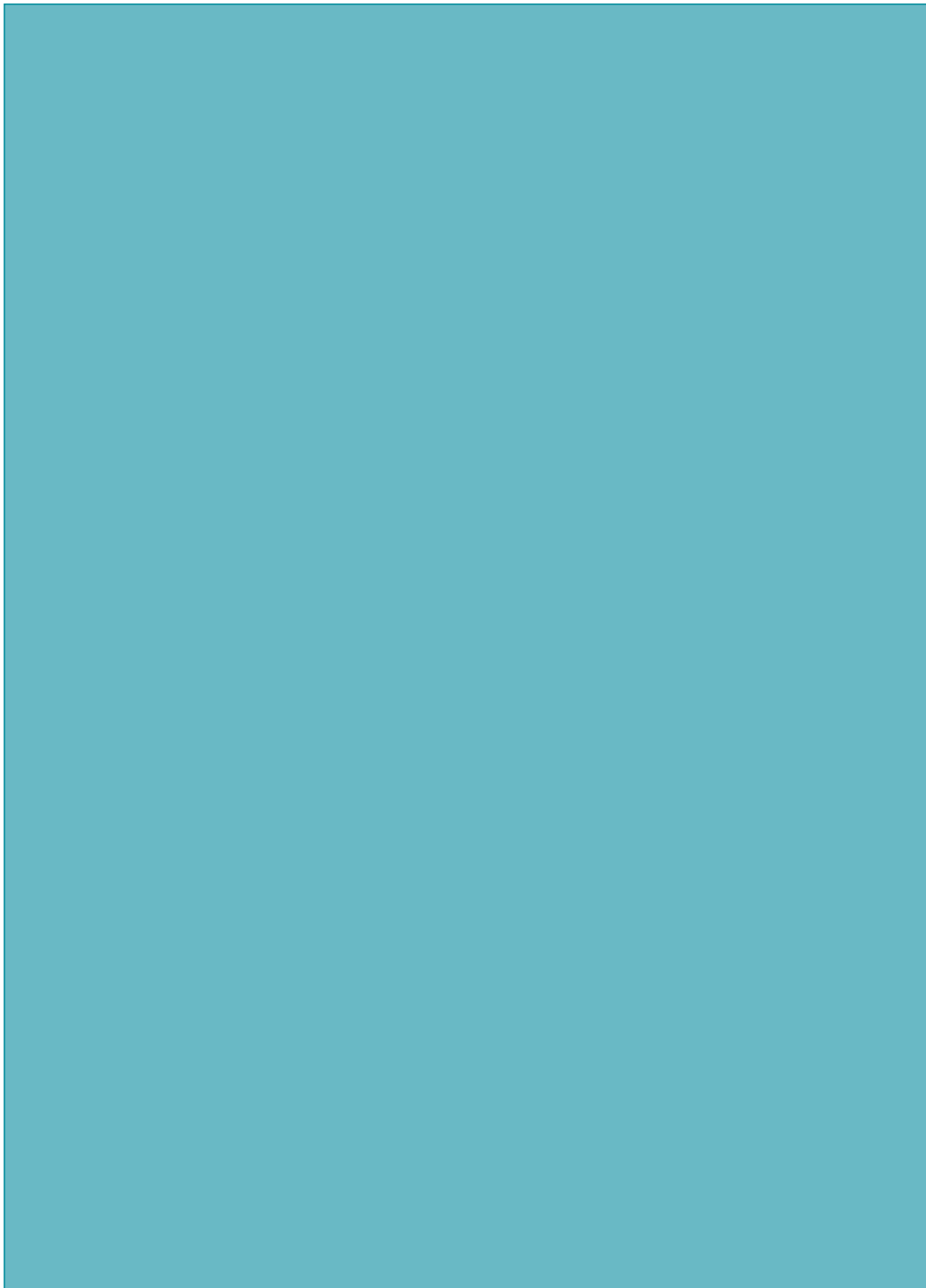
<u>IIN</u>	<u>Requesting Organization</u>	<u>Dissemination Instructions</u>
<p>Modes of transportation and conveyance (air, maritime, and ground)</p> <ul style="list-style-type: none"> - use of commercial transport/courier/shipping services and carriers - use of private/non-commercial carriers, couriers - types/identification of cargo containers; modifications - itineraries; favored routes; point of departure/source; nations transited - transshipment nodes; border-crossing techniques - multiple couriers chain-of-custody techniques; arrival/pick-up techniques <p>Finances of suspect groups</p> <ul style="list-style-type: none"> - support networks; state and private sponsors; shell companies - money-laundering techniques; unconventional financial transfers (e.g., hawalas) - shell companies; charity/humanitarian sponsors and covers - financial crime used to generate income; extortion of vulnerable targets - cooperative, facilitating financial institutions or service providers - financial links between public officials and criminal organizations or enterprises, hate groups, or FIS - criminal control of public, tribal financial assets or property <p>Impact of LE or USG efforts to combat suspect groups' activities</p> <ul style="list-style-type: none"> - infiltration; compromise; destruction; disruption - which tactics most/least effective; evidence of shift in suspect groups' tactics, techniques, or targets - effectiveness of LE efforts overseas 		

<u>IIN</u>	<u>Requesting Organization</u>	<u>Dissemination Instructions</u>
<ul style="list-style-type: none"> - response of suspect groups to LE efforts (countermeasures) - suspect group efforts at corruption of public/LE officials or employees - evidence of foreign/external LE entities' capabilities to cooperate and collaborate in joint efforts or operations - evidence of change in policies/attitudes overseas that affect tolerance for or freedom of action of suspect groups to operate in foreign environments <p>Recruitment; training; collaboration by suspect groups</p> <ul style="list-style-type: none"> - recruitment techniques and priority targets - training received: type, location, provider, curriculum, facilities <p>Tactics of intimidation, interference with free exercise of civil rights</p> <ul style="list-style-type: none"> - targets of hate groups, ethnic supremacist organizations - incidents of violence or incitement against individuals, groups, places of worship, schools, commercial entities identified with ethnic or political minorities <p>Capabilities, plans, intentions, MO of suspect groups to conduct computer intrusion or criminal assault on computer systems and data bases.</p> <p>Locally active hackers.</p>		

Federal Law Enforcement Intelligence

11

CHAPTER ELEVEN



Federal Law Enforcement Intelligence

Many federal agencies have reengineered their intelligence function since 9/11. Intelligence products have been redesigned or new products developed, dissemination methods have been revised, greater attention has been given to providing critical information that is unclassified for wide consumption by state, local, and tribal law enforcement (SLTLE), and new offices and initiatives have been developed. More information is being produced and disseminated more widely than in the history of law enforcement. Among the challenges that law enforcement now faces is accessing that needed information and using it with efficacy.

In many instances, federal intelligence initiatives are still in a dynamic state and, as a result, it is virtually impossible to provide an exhaustive discussion of them all. This chapter, therefore, will identify those federal intelligence resources of greatest use to SLTLE, their intelligence products, and the agencies' contact or access information. In addition, the chapter will present a broader discussion of the FBI than of other agencies because of the significant changes that have occurred in the FBI's structure and processes and the importance of the SLTLE/FBI relationship in counterterrorism and control of criminal enterprises.

While federal agencies have attempted to provide more unclassified information to America's law enforcement agencies, a significant amount of classified information remains relating to criminal investigations and terrorism. The FBI, therefore, has made a commitment to increase security clearances for SLTLE officers. Despite this, controversies and questions remain. As a result, dealing with the issue of classified information seems to be the first place to start when discussing intelligence from federal agencies.

181 <http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html> which amends a previous Executive Order on classified information.

Classified Information

There is often a mystique about classified information, leading most people after seeing a collection of classified documents to ask, "That's it?" For the most part, the key distinction between classified and unclassified information is that the former contains "sources and methods."

Some definitions: According to Executive Order 12958¹⁸¹ issued on March 23, 2003, information at the federal level may be classified at one of three levels:

- "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

- “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

When an intelligence analyst from the FBI, Drug Enforcement Administration (DEA), or other federal agency receives raw information, he or she must assess it for its source reliability and content validity. The “weight” of each of these variables and their corollaries provide significant insight into the credibility and importance of the information received. The higher the credibility and the greater the corroboration, the higher the “accuracy” of the information. Collectively, as credibility increases, the greater the need for a policy response.

For example, let us say that the FBI receives information about a possible terrorist attack. If the reliability and validity are very low, little credibility will be placed in the threat, although the FBI will develop corroboration and perhaps plan for a response. As validity and reliability increase, the greater credibility will result in devoting more resources to corroboration and a response. If validity and reliability are high, particularly if corroborated, the FBI will initiate a policy response. Policy responses may include proactive investigations, target hardening, and in the most severe cases, the Department of Homeland Security (DHS) may increase the threat level of the Homeland Security Advisory System (HSAS), triggering a significant string of policy responses at all levels of government. This admittedly oversimplified illustration demonstrates the need for analysts to know the sources and methods of information so that they can make the best judgments in their analysis.

Beyond analysts, it is important for investigators, too, to know sources and methods to work their leads. Members of the Joint Terrorism Task Forces (JTTF) need security clearances to conduct their investigations effectively. Do other members of SLTLE agencies need to have security clearances? Certainly not, but who receives a clearance depends on a number of factors. As a rule, SLTLE executives may apply for a clearance for three reasons:

1. To understand the complete nature of a threat within their jurisdiction.
2. To make management decisions, ranging from the assignment of personnel to investigations to the need for extending shifts and canceling officers' leaves should the threat condition warrant it.
3. As a courtesy to the executive who is contributing staff and resources to counterterrorism. This courtesy is not superficial, but aids the executive on matters of accountability.

For other members of an SLTLE agency, decisions should be made on a case-by-case basis to determine if the security clearance best serves the community's and, hence, national, interests. There are three reasons for not having an "open application" for security clearances. First, security clearance means having access to classified information. Before authorizing the application for a clearance, the agency should assess the applicant's "right to know" and "need to know" classified information should be considered. It may be reasonable to grant a security clearance to a local police detective who works organized crime cases; however, a traffic commander would have virtually no need for a clearance.

Second, the clearance process is labor intensive and expensive. It is simply not prudent fiscal management to authorize clearance investigations in all cases. Third, conducting an excess number of clearance investigations slows the process, thereby taking longer to process clearances for those persons who may be in more critical positions.

In most cases, the FBI will begin consideration of a clearance investigation for an SLTLE officer by examining local issues on a case-by-case basis.¹⁸² For those who seek to apply for a security clearance, the appropriate forms and fingerprint cards can be obtained from the local FBI Field Office. Appendix E describes the process for gaining a clearance and provides a list of frequently asked questions and their answers.¹⁸³

Sensitive But Unclassified (SBU) Information¹⁸⁴

Since it is not feasible for every law enforcement officer to have a security clearance, there is a mechanism to get critical information into the hands

182 The FBI provides the following guidance: Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. Local FBI Field Offices can help determine whether or not a security clearance is needed, and if so, what level is appropriate.

183 The National Security Clearance Application (Standard Form SF-86) can be downloaded from http://www.usaid.gov/procurement_bus_opp/procurement/forms/SF-86/sf-86.pdf.

184 As a means to aid in clarity, the FBI is moving away from the SBU label and using/will use Law Enforcement Sensitive in all cases, rather than using both labels.

of officers while not jeopardizing classified information: Declassifying the reports by removing sources and methods and labeling the report as SBU achieves this goal. This process is accomplished in two ways. One way is to use a “tear line” report in which an intelligence report has a segment,

Intelligence products have been redesigned or new products developed, DISSEMINATION methods have been revised, greater attention has been given to providing CRITICAL INFORMATION that is unclassified for wide consumption by SLTLE...

perhaps at the bottom of the page, where critical information is summarized and sources and methods are excluded. This portion of the report may be “torn off” (at least figuratively) and shared with persons who have a need to know the information but do not have a security clearance. The second method is to write intelligence products in a way that relays all critical information but excludes data that should remain classified. (The FBI Office of Intelligence is working specifically on this process.) Following this process, SLTLE officers receive documents that are labeled “Sensitive But Classified” or “Law Enforcement Sensitive”, thereby raising the question, “What does this mean?”

Over time some agencies have established procedures to identify and safeguard SBU information. Generally, this unclassified information is withheld from the public for a variety of reasons, but has to be accessible to law enforcement, private security, or other persons who have a responsibility to safeguard the public. The term SBU has been defined in various presidential-level directives and agency guidelines, but only indirectly in statute. Agencies have discretion to define SBU in ways that serve their particular needs to safeguard information. There is no uniformity in implementing rules throughout the federal government on the use of SBU.¹⁸⁵ There have been even fewer efforts to define and safeguard the information at the state, local, and tribal levels. There is an intuitive

185 For a detailed review of the SBU meaning and how it is defined and used by different statutes and regulations, see: Knezo, Genevieve J. *Sensitive But Unclassified” and Other Federal Security Controls on Scientific and Technical Information*. Washington, DC: Congressional Research Service.

understanding, but no formal process to control the information. Perhaps some guidance is being provided by the DHS which issued a directive in 2004 on “For Official Use Only” (FOUO) information.

DHS “For Official Use Only” (FOUO) Information

The FOUO label is used within DHS “...to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of a federal program, or other programs or operations essential to the national interest.”¹⁸⁶ FOUO is not classified information, but information that should be distributed only to persons who need to know the information to be aware of conditions that will help keep the homeland and, hence, the community, secure. Within DHS, the caveat “For Official Use Only” will be used to identify SBU information within the DHS community that is not otherwise governed by statute or regulation. At this point the designation applies only to DHS advisories and bulletins.

186 Department of Homeland Security, Management Directive System, MD Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. May 11, 2004.

187 Information in this section is based on interviews with FBI Office of Intelligence personnel, reviews of the Office of Intelligence Concepts of Operations (ConOps) and Congressional testimony of Director Mueller. See <http://www.fbi.gov/congress/congress04/mueller022404.htm>.

Since SLTLE agencies will encounter these labels when receiving federal intelligence products it is useful to know the framework from which they arise. At a practical level, the rule of thumb for law enforcement officers is to use good judgment when handling such materials. This does not mean that SLTLE officers may not disseminate this information further unless prohibited from doing so as indicated on the report. Rather, the officer should use the information in a manner that meets community safety needs, including disseminating portions of the information to those segments of the community that would benefit from the data contained in the report.

FEDERAL INTELLIGENCE PRODUCTS¹⁸⁷

In light of the perspective regarding classification of federal intelligence reports, the following discussions will describe federal intelligence products, virtually all of which will be SBU.

FBI Office of Intelligence

The FBI created the Office of Intelligence (OI) to establish and execute standards for recruiting, hiring, training, and developing the intelligence analytic work force, and ensuring that analysts are assigned to operational and field divisions in line with intelligence priorities. The FBI also established a new position, the executive assistant director for intelligence, who joins the three other executive assistant directors in the top tier of FBI management.¹⁸⁸ However, it is important to recognize that the OI goes far beyond being an analyst work force. Rather, it serves to provide centralized management of the FBI's intelligence capabilities and functions in the form of policy, standards, and oversight. Moreover, it embodies the Intelligence-Led Policing philosophy by serving as the driving force to guide operational activities.

To maximize the effectiveness of the intelligence process, the FBI's Office of Intelligence established a formal "intelligence requirements" process for identifying and resolving intelligence information (or information) needs. This is intended to identify key gaps—unanswered questions about a threat – in the FBI's collection capability that must be filled through targeted collection strategies.

¹⁸⁸ For more information on the FBI Office of Intelligence, see <http://www.fbi.gov/intelligence/intell.htm>.

In order to maximize the effectiveness of the intelligence process, the FBI OI has established a formal "INTELLIGENCE REQUIREMENTS" process for IDENTIFYING intelligence information (or information) needs and resolving them.

As a means to ensure that FBI-wide collection plans and directives are incorporated into field activities, every FBI Field Office has established a Field Intelligence Group (FIG). The FIG is the centralized intelligence component in each field office that is responsible for the management, execution, and coordination of intelligence functions. FIG personnel gather, analyze, and disseminate the intelligence collected in their field offices.

Staffed by both special agents and intelligence analysts, the FIG serves as the primary intelligence contact point for SLTLE agencies.

Field offices are also supporting the “24-hour intelligence cycle” of the FBI by using all appropriate resources to monitor, collect, and disseminate threat information, investigative developments (e.g., urgent reports), and other significant raw intelligence to meet the executive information needs of the field offices, other field offices, FBI Headquarters, Legal Attachés, and other federal or state and local agencies.

The reengineered FBI Office of Intelligence has developed two threat-based joint intelligence products and a third product known as the Intelligence Information Report. All of these products may be accessed by law enforcement at all levels of government.

189 The FIG should be contacted at your local FBI Field Office. Contact information for all field offices is at <http://www.fbi.gov/contact/fo/fo.htm>

- ***Intelligence Assessment:*** A comprehensive report on an intelligence issue related to criminal or national security threats within the service territory of an FBI Field Office. The assessment may be classified at any level or be unclassified depending on the nature of the information contained in the report. In most cases when the report is unclassified, it is Law Enforcement Sensitive.
- ***Intelligence Bulletin:*** A finished intelligence product in article format that describes new developments and evolving trends. The bulletins typically are SBU and available for distribution to state, local, and tribal law enforcement.
- ***Intelligence Information Report:*** Raw, unevaluated intelligence concerning “perishable” or time-limited information about criminal or national security issues. While the full IIR may be classified, state, local, and tribal law enforcement agencies will have access to SBU information in the report under the tear line.

An immediate source for FBI intelligence products is the Field Intelligence Group (FIG).¹⁸⁹ In addition, SLTLE agencies are able to gain direct access to these reports by secure email through Law Enforcement Online (LEO), the National Law Enforcement Telecommunications System (NLETS), or the Joint Regional Information Exchange System (JREIS). When circumstances warrant, the FBI and DHS will produce an intelligence product jointly and disseminate it to the appropriate agencies.

FBI Counterterrorism¹⁹⁰

Designated as the top priority for the FBI, countering terrorists' threats and acts is a responsibility requiring the integration of effective intelligence and operational capabilities. In support of the different intelligence units and activities discussed previously, the FBI has developed or enhanced a number of initiatives that seek to fulfill its counterterrorism mandate. While these are largely not intelligence programs per se, they all contribute to the intelligence cycle and consume intelligence for prevention and apprehension. A brief description of these initiatives will provide a more holistic vision of the FBI's counterterrorism strategy.

Specialized Counterterrorism Units

To improve its system for threat warnings, the FBI established a number of specialized counterterrorism units. They include the following:

- CT Watch, a 24-hour Counterterrorism Watch Center that serves as the FBI's focal point for all incoming terrorist threats
- The Communications Analysis Section analyzes terrorist electronic and telephone communications and identifies terrorist associations and networks
- The Document Exploitation Unit identifies and disseminates intelligence gleaned from million of pages of documents or computers seized overseas by intelligence agencies
- The Special Technologies and Applications Section provides technical support for FBI Field Office investigations requiring specialized computer technology expertise and support
- The interagency Terrorist Financing Operations Section is devoted entirely to the financial aspects of terrorism investigations and liaison with the financial services industry.

Intelligence gleaned from these special information and analysis resources is placed in the appropriate format (i.e., Bulletins, Assessments, IIR, advisories) and distributed to the field through appropriate dissemination avenues.

¹⁹⁰ Contact for the various counterterrorism program resources should be coordinated through your local FBI JTTF or FIG. The FBI Counterterrorism Division's comprehensive web page <http://www.fbi.gov/terrorinfo/counterterrorism/waronterrorhome.htm>.

FBI Information Sharing and Operational Coordination Initiatives

To defeat terrorists and their supporters, a wide range of organizations must work together. The FBI, therefore, has developed or refined both operational and support entities intended to bring the highest possible level of cooperation with SLTLE agencies, the Intelligence Community, and other federal government agencies.

- Joint Terrorism Task Forces (JTTF). Cooperation has been enhanced with federal, state, local, and tribal law enforcement agencies by significantly expanding the number of JTTFs. The task forces, which are operational in nature, tackle a wide array of potential terrorist threats and conduct investigations related to terrorist activities within the geographic region where the particular JTTF is headquartered.
- The National JTTF (NJTTF). In July 2002, the FBI established the NJTTF at FBI Headquarters and staffed it with representatives from 30 federal, state, and local agencies. The NJTTF acts as a “point of fusion” for terrorism information by coordinating the flow of information between Headquarters and the other JTTFs located across the country and between the agencies represented on the NJTTF and other government agencies.
- The Office of Law Enforcement Coordination (OLEC). The OLEC was created to enhance the ability of the FBI to forge cooperation and substantive relationships with all SLTLE counterparts. The OLEC, which is managed by FBI Assistant Director Louis Quijas, a former chief of police, also has liaison responsibilities with the DHS, COPS Office, Office of Justice Programs, and other federal agencies.

191 On August 28, 2004, President Bush announced: “I have ordered the establishment of a national counterterrorism center. This new center builds on the capabilities of the Terrorist Threat Integration Center, ... The center will become our government’s central knowledge bank for information about known and suspected terrorists, and will help ensure effective joint action across the government so that our efforts against terrorists are unified in priority and purpose. Center personnel will also prepare the daily terrorism threat report that comes to me and to senior government officials.” At this writing, no additional details were available.
<http://www.whitehouse.gov/news/releases/2004/08/20040828.html>

Terrorist Threat Integration Center (TTIC)¹⁹¹

The mission of TTIC is to enable full integration of terrorist threat-related information and analysis derived from all information and intelligence sources in the law enforcement and intelligence communities. The center is an interagency joint venture where officers will work together to provide a comprehensive, all-source-based picture of potential terrorist threats to

U.S. interests. TTIC's structure is designed to ensure rapid and unfettered sharing of relevant information across departmental lines by collapsing bureaucratic barriers and closing interjurisdictional seams. Elements of the DHS, FBI, Central Intelligence Agency (CIA), Department of Defense, and other federal government agencies form TTIC.

The center is an INTERAGENCY joint venture where officers will work together to provide a comprehensive, all-source-based picture of potential TERRORIST THREATS to U.S. interests.

On a daily basis, TTIC's interagency staff sifts through all-source reporting to identify terrorist plans of tactical concern as well as broader threat themes, which together help guide efforts to disrupt terrorist activities and enhance national security. TTIC also plays a key role in establishing a common threat picture by preparing daily threat assessments and updates for the President and the Departments of Defense, State, and Homeland Security, as well as the broader Intelligence Community, and by creating a consolidated website for the counterterrorism community. The center is colocated with counterterrorism elements from the CIA and FBI, further enhancing coordination efforts.

TTIC is not operational and does not collect intelligence; rather, it receives collected intelligence from other agencies (FBI, CIA, etc.) and analyzes the integrated raw information. While not dealing directly with field components of the FBI or SLTLE, the products disseminated by TTIC serve as an important source for threat development and prevention.

Terrorist Screening Center (TSC)¹⁹²

The TSC was created to ensure that government investigators, screeners, agents, and state and local law enforcement officers have ready access to the information and expertise they need to respond quickly when a suspected terrorist is screened or stopped. The TSC consolidates access to terrorist watch lists from multiple agencies and provide 24/7 operational

192 Information for this section was gained from interviews and reviews of various courses, including testimony and press releases at <http://www.fbi.gov/congress/congress04/bucella012604.htm>, <http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm>, and http://www.odci.gov/cia/public-affairs/speeches/2003/wiley_speech_02262003.html.

support for thousands of federal screeners and state and local law enforcement officers across the country and around the world. The intent of the TSC is to ensure that federal, state, and local officials are working off of the same unified, comprehensive set of antiterrorist information. Since its implementation on December 1, 2003, the TSC has provided the following:

- A single coordination point for terrorist screening data
- A consolidated 24/7 call center for encounter identification assistance
- A coordinated law enforcement response to federal, state, and local law enforcement
- A formal process for tracking encounters and ensuring that feedback is supplied to the appropriate entities.

The TSC created the terrorist screening database (TSDB), a single, comprehensive source of known or appropriately suspected international and domestic terrorists. These data are available to local, state, and federal law enforcement officers through the National Crime Information Center (NCIC). When a police officer queries the NCIC, he or she may receive a notification that the query resulted in the potential match of a record within the TSDB and the officer is directed to contact the TSC to determine if it is an actual match. If it is an actual match, the TSC transfers the call to the FBI's CT Watch to provide operational guidance to the officer.

Consolidated Terrorist Screening Database

The TSC receives international and domestic terrorist identity records and maintains them in its consolidated TSDB. The TSC reviews each record to determine which are eligible for entry into the NCIC's Violent Gang and Terrorist Organization File (VGTOF) and once the record is entered into NCIC, it is accessible by state, local, and federal law enforcement officers. If a query by a law enforcement officer matches a name in NCIC, the officer will be requested, through the NCIC printout, to contact the TSC. The printout also provides the officer with instructions to arrest, detain, question, or release the subject. If the TSC determines that the person encountered by the officer is a match with a person in the NCIC/VGTOF file, the officer is immediately connected to the FBI's CT Watch for operational

guidance. Depending on the situation, the CT Watch may dispatch a local JTTF agent to assist the law enforcement officer. Information that the officer obtained through the encounter is then sent back to the originating agency.

An example will illustrate the TSC's processes. On August 20, 2004, as two off-duty police officers were traveling across the Chesapeake Bay Bridge, they observed individuals filming the structure of the bridge. The officers reported this suspicious activity to the Maryland Transportation Authority (MTA) who then conducted a traffic stop of the vehicle. The MTA officers ran an NCIC check on one of the occupants of the car and learned that the individual may have a record within the TSDB. At the NCIC's request, the officers contacted the TSC and learned that the individual was the subject of the TSDB record. The TSC transferred the call to the FBI's CT Watch who informed the MTA that the individual an alleged coconspirator in a significant terrorism case. The FBI arrested the subject on a material witness warrant, and a search warrant executed at the subject's residence turned up valuable evidence. This new level of information sharing and cooperation among state, local, and federal law enforcement agencies enhances our ability to prevent a terrorist attack within the United States.

193 The intelligence component of DHS is in the Information Analysis and Infrastructure Protection (IAIP) Directorate: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml. For current information on DHS threats and security, see http://www.dhs.gov/dhspublic/theme_home6.jsp.

Department of Homeland Security¹⁹³

The DHS, through the Directorate of Information Analysis and Infrastructure Protection (IAIP), will merge the capability to identify and assess current and future threats to the homeland, map those threats against our vulnerabilities, issue timely warnings, and take preventive and protective action.

Intelligence Analysis and Alerts

Actionable intelligence, that is, information that can lead to stopping or apprehending terrorists, is essential to the primary mission of DHS. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve the government's ability to disrupt and prevent terrorist acts and to provide useful warning to the private sector and our population. The IAIP Directorate will fuse and analyze information from multiple sources pertaining to terrorist threats. The DHS

will be a full partner and consumer of all intelligence-generating agencies, such as the National Security Agency, the CIA, and the FBI.

The DHS's threat analysis and warning functions will support the President and, as he directs, other national decision makers responsible for securing the homeland from terrorism. It will coordinate and, as appropriate, consolidate the federal government's lines of communication with state and local public safety agencies and with the private sector, creating a coherent and efficient system for conveying actionable intelligence and other threat information. The IAIP Directorate also administers the HSAS.

Critical Infrastructure Protection

The attacks of September 11 highlighted the fact that terrorists are capable of causing enormous damage to our country by attacking our critical infrastructure; food, water, agriculture, and health and emergency services; energy sources (electrical, nuclear, gas and oil, dams); transportation (air, road, rail, ports, waterways); information and telecommunications networks; banking and finance systems; postal services; and other assets and systems vital to our national security, public health and safety, economy, and way of life.

Protecting America's critical infrastructure is the shared responsibility of federal, state, and local government, in active partnership with the private sector, which owns approximately 85 percent of our nation's critical infrastructure. The IAIP Directorate will take the lead in coordinating the national effort to secure the nation's infrastructure. This will give state, local, and private entities one primary contact instead of many for coordinating protection activities within the federal government, including vulnerability assessments, strategic planning efforts, and exercises.

Cyber Security

Our nation's information and telecommunications systems are directly connected to many other critical infrastructure sectors, including banking and finance, energy, and transportation. The consequences of an attack on our cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and

imperiling public safety. The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, the IAIP Directorate places an especially high priority on protecting our cyber infrastructure from terrorist attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the former National Infrastructure Protection Center (FBI). The IAIP Directorate will augment those capabilities with the response functions of the National Cyber Security Division (NCSA) United States Computer Emergency Response Team (US-CERT).¹⁹⁴ Because our information and telecommunications sectors are increasingly interconnected, DHS will also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.

Indications and Warning Advisories

In advance of real-time crisis or attack, the IAIP Directorate will provide the following:

- Coordinated DHS-FBI threat warnings and advisories against the homeland, including physical and cyber events¹⁹⁵
- Processes to develop and issue national and sector-specific threat advisories through the HSAS
- Terrorist threat information for release to the public, private industry, or state and local governments.

Figure 11-1 illustrates DHS and intelligence and threat assessment processes. DHS-FBI advisories are produced in several forms. Figures 11-2, 11-3, 11-4, and 11-5 are illustrations of DHS advisory templates. SLTLE agencies have access to these advisories through the various secure law enforcement email systems (i.e., NLETS, LEO, JRIES, Regional Information Sharing Systems [RISS.net], Anti-Terrorism Information Exchange [ATIX]).

194 <http://www.us-cert.gov>

195 http://www.dhs.gov/dhspublic/verify_redirect.jsp?url=http://www.us-cert.gov&title=cyber+events

Figure 11-1: DHS and Intelligence and Threat Assessment Processes



Figure 11-2: DHS Operations Morning Brief

UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE



WARNING: This document is FOR OFFICIAL USE ONLY. This information shall not be distributed beyond the original addressees without prior authorization of the originator. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Homeland Security Operations Morning Brief DD Month YYYY


Overnight Developments

1. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DD MM YY, HSOC initiated name checks. (CBP Morning Report __ MM YY __; HSOC __)
2. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DD MM YY, HSOC initiated name checks. (CBP Morning Report __ MM YY __; HSOC __)
3. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DD MM YY, HSOC initiated name checks. (CBP Morning Report __ MM YY __; HSOC __)
4. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DD MM YY, HSOC initiated name checks. (CBP Morning Report __ MM YY __; HSOC __)
5. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DD MM YY, HSOC initiated name checks. (CBP Morning Report __ MM YY __; HSOC __)

Page 1 of 1

Homeland Security Operations Morning Brief dd Month YYYY
UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE
Third Agency Dissemination of This Material is prohibited Without Prior DHS Approval.
This document is for deterring, detecting, and preventing terrorism. It contains law enforcement sensitive material and may be shared appropriately, but should be protected from public dissemination.

Figure 11-3: DHS Information Bulletin

	Information Bulletin Title: _____ Date: _____
<p>LIMITED DISTRIBUTION: Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without the express approval of the Department of Homeland Security (DHS). This information is intended for entities identified on the attention line below. All requests for further distribution must be submitted to the DHS Information Management and Requirements Division at 202-282-8168. After business hours contact the DHS Homeland Security Operations Center at Phone (202) 282-8101.</p> <p>ATTENTION: Provide guidance as to who within an organization may have primary responsibility for taking action on this product. Examples: Physical Security Officers, Facility Managers, etc.</p> <p>OVERVIEW Provide a concise summation of the information in the bulletin, a disclaimer as to the intention of the product, and any limitations as to the further dissemination of this product by the intended recipients.</p> <p>Homeland Security Information Bulletins are informational in nature and are designed to provide updates on the training, tactics, or strategies of terrorists.</p> <p>DHS Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.</p> <p>DETAILS [This section provides the DHS assessment of the information, any recommendations or resultant changes to procedures or processes, and any other applicable information for the consumer.]</p> <p>SUGGESTED PROTECTIVE MEASURES [This section provides the DHS recommended protective actions for immediate implementation, including best practices when available.]</p> <p>Concluding paragraphs:</p> <p>DHS encourages recipients of this Information Bulletin to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.</p> <p>DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.</p>	

Information Bulletin

Figure 11-4: DHS Physical Advisory



Advisory

Title: _____
Date: _____

LIMITED DISTRIBUTION: Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without the express approval of the Department of Homeland Security (DHS). This information is intended for entities identified on the attention line below. All requests for further distribution must be submitted to the DHS Information Management and Requirements Division at 202-282-8168. After business hours contact the DHS Homeland Security Operations Center at Phone (202) 282-8101.

ATTENTION: Provide guidance as to who within an organization may have primary responsibility for taking action on this product. Examples: Physical Security Officers, Facility Managers, etc.

OVERVIEW

Provide one or two sentences in the form of an executive summary of the warning. This may be all a recipient reviews upon initial notification due to the limited storage or viewing capacities of electronic paging devices.

DETAILS

This section provides the DHS assessment of the threat, recommendations and solutions for handling the issue, and any other applicable information for the consumer.

SUGGESTED PROTECTIVE MEASURES

This section provides the DHS recommended protective actions for immediate implementation, including best practices when available.


Concluding paragraphs:

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.

Protecting America's CRITICAL INFRASTRUCTURE is the shared responsibility of FEDERAL, STATE, and LOCAL government, in active PARTNERSHIP with the private sector...

Figure 11-5: DHS Cyber Advisory



Advisory
Title: _____
Date: _____

SYSTEMS AFFECTED [Insert list of systems affected by the threat/vulnerability]

OVERVIEW
[Insert a concise synopsis/summary of the threat/vulnerability.]

IMPACT
[The severity of the threat against the affected system(s) depends upon one or more of the following:
- widespread use of the affected system(s)
- mission criticality of the applications running on affected system(s)
- type(s) of affected system(s).
Available analysis of potential or realized impacts will be inserted here.]

DETAILS
[Insert authorized details on the threat/vulnerability.]

SUGGESTED PROTECTIVE MEASURES
DHS is working with other government agencies, network security experts, and industry representatives to define, prioritize, and mitigate these vulnerabilities. DHS encourages implementation of industry best practices. Additionally, the following suggested workarounds and other mitigation steps are provided:

[Insert detailed threat and vulnerability steps including locations for obtaining patches and vulnerability assessments if available.]

Concluding paragraphs:

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.

Drug Enforcement Administration¹⁹⁶

Since its establishment in 1973, the DEA, in coordination with other federal, state, local, and foreign law enforcement organizations, has been responsible for the collection, analysis, and dissemination of drug-related intelligence. The role of intelligence in drug law enforcement is critical. The DEA Intelligence Program helps initiate new investigations of major drug organizations, strengthens ongoing investigations and subsequent prosecutions, develops information that leads to seizures and arrests, and provides policy makers with drug trend information on which they can base programmatic decisions. The specific functions of the DEA's intelligence mission are as follows:

- Collect and produce intelligence in support of the administrator and other federal, state, and local agencies
- Establish and maintain close working relationships with all agencies that produce or use narcotics intelligence
- Increase the efficiency in the reporting, analysis, storage, retrieval, and exchange of such information;
- Undertake a continuing review of the narcotics intelligence effort to identify and correct deficiencies.

The DEA's Intelligence Program has grown significantly since its inception. From only a handful of intelligence analysts (I/A) in the domestic offices and Headquarters in 1973, the total number of intelligence analysts worldwide is now more than 680. DEA's intelligence Program consists of several entities that are staffed by both intelligence analysts and special agents: Intelligence groups and functions in the domestic field divisions, district, resident and foreign offices, the El Paso Intelligence Center, and the Intelligence Division at DEA Headquarters. Program responsibility for the DEA's intelligence mission rests with the DEA assistant administrator for intelligence.

196 A number of DEA Strategic Intelligence Reports are available online at <http://www.dea.gov/pubs/intel.htm>. For other intelligence reports and related information, contact your nearest DEA Field Office <http://www.dea.gov/agency/domestic.htm#caribbean>.

Legislation and presidential directives and orders have expanded the role of the Intelligence Community and the Department of Defense in the anti-drug effort. DEA interaction with both components occurs on a daily basis in the foreign field and at Headquarters. At the strategic intelligence level, the Intelligence Division participates in a wide range of interagency assessment and targeting groups that incorporate drug intelligence from the antidrug community to provide policymakers with all-source drug trend and trafficking reporting.

With analytical support from the Intelligence Program, DEA has disrupted major trafficking organizations or put them entirely out of business. The DEA Intelligence Division also cooperates a great deal with state and local law enforcement and will soon provide intelligence training for state, local, federal, and foreign agencies. This training will be held at the Justice Training Center in Quantico, Virginia, and will address the full spectrum of drug intelligence training needs. The best practices and theories of all partners in working the drug issue will be solicited and incorporated into the training. Academic programs, the exchange of federal, state, and local drug experience, and the sharing of, and exposure to, new ideas will result in more effective application of drug intelligence resources at all levels. The DEA divides drug intelligence into three broad categories: tactical, investigative, and strategic.

- Tactical intelligence is evaluated information on which immediate enforcement action – arrests, seizures, and interdictions – can be based.
- Investigative intelligence provides analytical support to investigations and prosecutions to dismantle criminal organizations and gain resources.
- Strategic intelligence focuses on the current picture of drug trafficking from cultivation to distribution that can be used for management decision making, resource deployment, and policy planning.

197 See <http://www.usdoj.gov/dea/pubs/intel.htm>.

Intelligence Products

Tactical and investigative intelligence is available to SLTLE agencies through the local DEA field office. In addition, intelligence can be shared with state, local, and tribal agencies through secure email. Many strategic intelligence reports are available on the DEA website.¹⁹⁷ Reports that are “Law Enforcement Sensitive” can be obtained through the local DEA office.

El Paso Intelligence Center (EPIC)¹⁹⁸

The El Paso Intelligence Center (EPIC) was established in 1974 in response to a Department of Justice study. The study, which detailed drug and border enforcement strategy and programs, proposed the establishment of a southwest border intelligence service center staffed by representatives of the Immigration and Naturalization Service, the U.S. Customs Service, and the DEA. The original EPIC staff comprised 17 employees from the three founding agencies. Initially, EPIC focused on the U.S.-Mexico border and its primary interest was drug movement and immigration violations.

Today, EPIC still concentrates primarily on drug movement and immigration violations. Because these criminal activities are seldom limited to one geographic area, EPIC's focus has broadened to include all of the United States and the Western Hemisphere where drug and alien movements are directed toward the United States. Staffing at the DEA-led center has increased to more than 300 analysts, agents, and support personnel from 15 federal agencies, the Texas Department of Public Safety, and the Texas Air National Guard. Information-sharing agreements with other federal law enforcement agencies, the Royal Canadian Mounted Police, and each of the 50 states ensure that EPIC support is available to those who need it. A telephone call, fax, or email from any of these agencies provides the requestor with real-time information from different federal databases, plus EPIC's own internal database.

In addition to these services, a number of EPIC programs are dedicated to post-seizure analysis and the establishment of links between recent enforcement actions and ongoing investigations. EPIC also coordinates training for state and local officers in the methods of highway drug and drug currency interdiction through its Operation Pipeline program. In addition, EPIC personnel coordinate and conduct training seminars throughout the United States, covering such topics as indicators of trafficking and concealment methods used by couriers.

In a continuing effort to stay abreast of changing trends, EPIC has developed the National Clandestine Laboratory Seizure Database. EPIC's future course will be driven by the National General Counterdrug

198 See <http://www.dea.gov/programs/epic.htm>.

Intelligence Plan, as well. As a major national center in the new drug intelligence architecture, EPIC will serve as a clearinghouse for the High-Intensity Drug Trafficking Areas (HITDA) Intelligence Centers, gathering state and local law enforcement drug information and providing drug intelligence back to the HIDTA Intelligence Centers.

National Drug Pointer Index (NDPIX) and National Virtual Pointer System (NVPS)¹⁹⁹

For many years, state and local law enforcement envisioned a drug pointer system that would allow them to determine if other law enforcement organizations were investigating the same drug suspect. The DEA was designated by the Office of National Drug Control Policy in 1992 to take the lead in developing a national drug pointer system to assist federal, state, and local law enforcement agencies investigating drug trafficking organizations and to enhance officer safety by preventing duplicate investigations. The DEA drew from the experience of state and local agencies to make certain that their concerns were addressed and that they had extensive input and involvement in the development of the system.

199 See <http://www.dea.gov/programs/ndpix.htm>.

The National Law Enforcement Telecommunications System (NLETS)-a familiar, fast, and effective network that reaches into almost every police entity in the United States-is the backbone of the NDPIX.

The National Drug Pointer Index (NDPIX) became operational across the United States in October 1997. The National Law Enforcement Telecommunications System (NLETS)-a familiar, fast, and effective network that reaches into almost every police entity in the United States-is the backbone of the NDPIX. Participating agencies are required to submit active case-targeting information to NDPIX to receive pointer information from the NDPIX. The greater the number of data elements entered, the greater the likelihood of identifying possible matches. Designed to be a

true pointer system, the NDPIX merely serves as a “switchboard” that provides a vehicle for timely notification of common investigative targets. The actual case information is shared only when telephonic contact is made between the officers or agents who have been linked by their entries into the NDPIX.

NDPIX was developed to: (1) promote information sharing; (2) facilitate drug-related investigations; (3) prevent duplicate investigations; (4) increase coordination among federal, state, and local law enforcement agencies; and (5) enhance the personal safety of law enforcement officers. At this writing, NDPIX is being transitioned and upgraded to the National Virtual Pointer System (NVPS). A steering committee—which included DEA, HIDTA, RISS, the National Drug Intelligence Center (NDIC), the National Institute of Justice (NIJ), the National Sheriff’s Association (NSA), the International Association of Chiefs of Police (IACP), and the National Alliance of State Drug Enforcement Agencies (NASDEA)—developed the specifications for the system and is overseeing its testing and transition.

Characteristics of the NVPS will include the following:

- It will cover all crimes, not just drugs.
- The system will accept only targets of open investigations with assigned case numbers.
- Transaction formats will contain an identifying field for the NVPS Identifier.
- It will use a secure telecommunications network.
- It will use the NDPIX “Mandatory” data elements.
- A single sign-on from any participant will allow access to all participating pointer databases.
- Each system will provide a userid and password to its respective users.
- Each system will maintain its own data.
- Uniform Crime Reporting (UCR) or the National Incident-Based Reporting System (NIBRS) codes will be used to identify type of crime.
- The system will target deconfliction for all crimes.
- It will rely on web-based communications.
- NVPS will have links with HIDTA and RISS.

An important aspect of the links with NVPS will be that NDPIX participants will continue to use their existing formats and procedures for entries, updates, and renewals and NDPIX notifications will continue in the same formats. The transition to NVPS will be seamless. This change represents an important upgrade to networked intelligence that can be of value to all law enforcement agencies.

National Drug Intelligence Center (NDIC)²⁰⁰

The National Drug Intelligence Center (NDIC), established in 1993, is a component of the U.S. Department of Justice and a member of the Intelligence Community. The General Counterdrug Intelligence Plan, implemented in February 2000, designated NDIC as the nation's principal center for strategic domestic counterdrug intelligence. The intent of NDIC is to meet three fundamental missions:

- To support national policymakers and law enforcement decision makers with strategic domestic drug intelligence
- To support Intelligence Community counterdrug efforts
- To produce national, regional, and state drug threat assessments.

The Intelligence Division consists of six geographic units and four specialized units. The six geographic units correspond to the regions of the Department of Justice Organized Crime Drug Enforcement Task Force (OCDETF)²⁰¹ program and concentrate on drug trafficking and abuse. The four specialized units include the Drug Trends Analysis Unit, the Organized Crime and Violence Unit, the National Drug Threat Assessment Unit, and the National Interdiction Support Unit.

Within the geographic units, NDIC intelligence analysts cover each state and various U.S. territories. Intelligence analysts maintain extensive contacts with federal, state, and local law enforcement and Intelligence Community personnel in all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, and the Pacific territories of Guam, American Samoa, and the Northern Mariana Islands. NDIC collaborates with other agencies such as the DEA, FBI, U.S. Coast Guard, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Bureau of Prisons, and the Office of

²⁰⁰ See <http://www.usdoj.gov/ndic/>.

²⁰¹ While the OCDETFs are operational, not intelligence entities, they are not only consumers of intelligence, but are also sources for information collection. For more information see <http://www.usdoj.gov/dea/programs/ocdetf.htm>.

National Drug Control Policy (ONDCP). NDIC is one of four national intelligence centers including the EPIC, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), and the DCI Crime and Narcotics Center (CNC). NDIC also works closely with the High Intensity Drug Trafficking Areas (HIDTAs) and the OCDETF.

Intelligence Products

Threat assessments, NDIC's primary intelligence products, provide policy makers and counterdrug executives with timely, predictive reports of the threat posed by illicit drugs in the United States.

- The *National Drug Threat Assessment*, NDIC's major intelligence product, is a comprehensive annual report on national drug trafficking and abuse trends within the United States. The assessment identifies the primary drug threat to the nation, monitors fluctuations in consumption levels, tracks drug availability by geographic market, and analyzes trafficking and distribution patterns. The report highlights the most current quantitative and qualitative information on availability, demand, production and cultivation, transportation, and distribution, as well as the effects of a particular drug on abusers and society as a whole.
- *State Drug Threat Assessment* provides a detailed threat assessment of drug trends within a particular state. Each report identifies the primary drug threat in the state and gives a detailed overview of the most current trends by drug type.
- *Information Bulletins* are developed in response to new trends or high-priority drug issues. They are relayed quickly to the law enforcement and intelligence communities and are intended to warn law enforcement officials of emerging trends.

202 See <http://www.whitehousedrugpolicy.gov/hidta/> for HIDTA points of contact.

High-Intensity Drug Trafficking Areas (HIDTA) Regional Intelligence Centers²⁰²

The HIDTA Intelligence System has more than 1,500 law enforcement personnel, mostly criminal intelligence analysts, participating full time in more than 60 intelligence initiatives in the 28 HIDTA designated areas

throughout the United States. While HIDTA is a counterdrug program, the intelligence centers operate in a general criminal intelligence environment, thereby leveraging all criminal intelligence information for the program's primary mission.²⁰³

The HIDTA Intelligence System, a core element in the creation and growth of many SLTLE intelligence programs, largely depends on HIDTA program mandates. Each HIDTA must establish an intelligence center comanaged by a federal and a state or local law enforcement agency. The core mission of each individual HIDTA Intelligence Center is to provide tactical, operational, and strategic intelligence support to its HIDTA executive board, a group of participating law enforcement agency principals responsible for the daily management of their respective HDTAs, HIDTA-funded task forces, and other regional HDTAs. Developing regional threat assessments and providing event and target deconfliction are also among the centers' core missions. These core functions are critical to building trust and breaking down parochialism between and among the local, state, and federal participating law enforcement agencies.

The plan to connect all HIDTA Intelligence Centers through RISS.net was initiated by the HIDTA Program Office at ONDCP in 1999 and completed in mid-2003. The HIDTA Program Office has commissioned interagency and interdisciplinary working committees to develop a national information-sharing plan, focusing on issues relating to legal, agency policy, privacy, technical, and logistical information-sharing matters. HIDTA program and committee personnel are coordinating with, and implementing recommendations made by, other information-sharing initiatives such as Global, Matrix, and federally sponsored intelligence programs.²⁰⁴

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)²⁰⁵

The Intelligence Division of ATF has evolved rapidly as an important tool for the diverse responsibilities of the bureau. Several activities in particular demonstrate the intelligence capability and resources of ATF.

203 http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=139&issue_id=11200

204 As an illustration of the comprehensive and integrated nature of the HIDTA programs and intelligence centers, see <http://www.ncjrs.org/ondcpublications/enforce/hidta2001/ca-fs.html>.

205 Contact your local ATF Field Office for Intelligence Products and resources. Offices and contact information can be found at <http://www.atf.gov/field/index.htm>.

The ATF, which is now an agency of the Department of Justice, has developed Field Intelligence Groups at each of its 23 Field Divisions strategically located throughout the United States. These intelligence groups meld the training and experience of special agents, intelligence research specialists, industry operations inspectors, and support staff who focus on providing tactical intelligence support for their respective field divisions and their external law enforcement partners. Each Field Intelligence Group works under the authority of a supervisory special agent. The intelligence group supervisors are coordinated by, and work in conjunction with, the Intelligence Division to form a bureau-wide intelligence infrastructure. The Intelligence Division has provided indoctrination and training for all Field Intelligence Group supervisors, intelligence officers, and intelligence research specialists.

... the [ATF] Intelligence Division spearheaded the formulation of an MOU with the FBI to collaborate on investigations conducted by **JOINT TERRORISM TASK FORCES** located throughout the United States.

ATF maintains intelligence partnerships with the NDIC, EPIC, FinCEN, INTERPOL, the Federal Bureau of Investigation Counter Terrorism Center, (FBI/CTC) and other international intelligence sources. Furthermore, ATF maintains a memorandum of understanding (MOU) with the six Regional Information Sharing Systems (RISS) that represent thousands of SLTLE agencies, pledging to share unique and vital intelligence resources. These external partners are key components of ATF's Strategic Intelligence Plan and the means by which ATF ensures a maximum contribution to the nation's law enforcement and intelligence communities.

During FY 2000, the Intelligence Division spearheaded the formulation of an MOU with the FBI to collaborate on investigations conducted by Joint Terrorism Task Forces located throughout the United States. This MOU brings ATF's unique knowledge and skills of explosives and firearms violations to the FBI's expertise in terrorism.

The Intelligence Division has implemented a state-of-the-art automated case management/ intelligence reporting system called N-FOCIS (National Field Office Case Information System). The system consists of two companion applications: N-FORCE for special agents and N-SPECT for industry operations inspectors. Both eliminate redundant manual data entry on hard copy forms and provide a comprehensive reporting and information management application in a secure electronic environment.

N-FOCIS constitutes an online case management system and electronic central information repository that allows ATF to analyze and fully exploit investigative intelligence. N-FOCIS epitomizes the strength and unique value of ATF's combined criminal and industry operations enforcement missions. The Intelligence Division has provided in-service training to many of the ATF field division special agents, investigative assistants, and inspectors on the use of the N-FOCIS applications. ATF is planning to expand the N-FOCIS functionality and to integrate N-FOCIS with several key ATF applications including the National Revenue Center, the National Tracing Center, National Arson and Explosive Repository, and the Intelligence Division's Text Management System. This integration plan establishes N-FOCIS as the bureau's information backbone.

206 As an illustration see <http://www.atf.gov/field/newyork/rcgc/index.htm>.

207 See <http://www.fincen.gov/>.

The Intelligence Division prepares a wide range of strategic intelligence reports related to the ATF mission that are available to SLTLE. In addition, intelligence is shared with state and local agencies through RISS and the JTTFs. In addition, ATF will readily respond to inquiries wherein SBU information may be shared.

ATF has also created a series of Regional Crime Gun Centers. The intent of the centers is to integrate gun tracing with ATF intelligence as well as with the HIDTA Regional Intelligence Centers to suppress gun-related crime.²⁰⁶

Financial Crimes Enforcement Network (FinCEN)²⁰⁷

The Financial Crimes Enforcement Network (FinCEN) is a network designed to bring agencies, investigators, and information together to fight the complex problem of money laundering. Since its creation in 1990, FinCEN

has worked to maximize information sharing among law enforcement agencies and its other partners in the regulatory and financial communities. Through cooperation and partnerships, FinCEN's network approach encourages cost-effective and efficient measures to combat money laundering domestically and internationally.

The network supports federal, state, local, tribal, and international law enforcement by analyzing information required under the Bank Secrecy Act (BSA), one of the nation's most important tools in the fight against money laundering. The BSA's record keeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities, and their assets. Over the years, FinCEN staff has developed its expertise in adding value to the information collected under the BSA by uncovering leads and exposing unknown pieces of information contained in the complexities of money laundering schemes.

Illicit financial transactions can take many routes – some complex, some simple, but all increasingly inventive – with the ultimate goal being to disguise its source. The money can move through banks, check cashers, money transmitters, businesses, casinos, and is often sent overseas to become “clean.” The tools of the money launderer can range from complicated financial transactions, carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

Intelligence research specialists and law enforcement support staff research and analyze this information and other critical forms of intelligence to support financial criminal investigations. The ability to network with a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country. Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its employees—a responsibility that strongly imprints all of its data management functions and operations.

FinCEN's information sources fall into three categories:

- ***Financial Database:*** The financial database consists of reports that the BSA requires to be filed, such as data on large currency transactions

conducted at financial institutions or casinos, suspicious transactions, and international movements of currency or negotiable monetary instruments. This information often provides invaluable assistance for investigators because it is not readily available from any other source and preserves a financial paper trail for investigators to track criminals' proceeds and their assets.

- **Commercial Databases:** Information from commercially available sources plays an increasingly vital role in criminal investigations. Commercial databases include information such as state, corporation, property, and people locator records, as well as professional licenses and vehicle registrations.
- **Law Enforcement Databases:** FinCEN is able to access various law enforcement databases through written agreements with each agency.

FinCEN works closely with the International Association of Chiefs of Police (IACP), National Association of Attorneys General (NAAG), National White Collar Crime Center (NW3C), and other organizations to inform law enforcement about the information that is available at FinCEN and how to use that information to attack criminal proceeds.

208 See http://www.fincen.gov/le_hifca_design.html.

High Risk Money Laundering and Related Financial Crimes Areas (HIFCA)²⁰⁸

HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high intensity money laundering zones. HIFCAs may be defined geographically or they can also be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

The HIFCA program is intended to concentrate law enforcement efforts at the federal, state, and local levels to combat money laundering in designated high-intensity money laundering zones. To implement this goal, a money laundering action team will be created or identified within each HIFCA to spearhead a coordinated federal, state, and local antimoney laundering effort. Each action team will: (1) be composed of all relevant

federal, state, and local enforcement authorities, prosecutors, and financial regulators; (2) focus on tracing funds to the HIFCA from other areas, and from the HIFCA to other areas so that related investigations can be undertaken; (3) focus on collaborative investigative techniques, both within the HIFCA and between the HIFCA and other areas; (4) ensure a more systemic exchange of information on money laundering between HIFCA participants; and (5) include an asset forfeiture component as part of its work.

Gateway

FinCEN's Gateway system enables federal, state, and local law enforcement agencies to have online access to records filed under the BSA. The system saves investigative time and money by enabling investigators to conduct their own research and analysis of BSA data rather than relying on the resources of an intermediary agency to obtain financial records. A unique feature of Gateway is the “query alert” mechanism that automatically signals FinCEN when two or more agencies have an interest in the same subject. In this way, FinCEN is able to assist participating agencies in coordinating their investigations.

Virtually every criminal enterprise and terrorist organization is involved in some dimension of money laundering. The complexities of forensic accounting, often complicated by jurisdictional barriers, reinforces the need for intelligence personnel to be aware of the resources and expertise available through FinCEN.

CONCLUSION

As demonstrated in this chapter, the amount of information and intelligence being generated by federal law enforcement agencies is significant. If that information is not being used, then its value is lost. Not only are federal agencies responsible for making information available to SLTLE agencies in an accessible and consumable form, nonfederal law enforcement must develop the mechanisms for receiving the information and to be good consumers of it.

One of the ongoing controversies is the problem of dealing with classified information. This chapter explained the classification process as well as the initiatives that are being undertaken to deal with this issue. One measure is to increase the number of security clearances for SLTLE personnel. The other measure is for the FBI to write intelligence reports so that they are unclassified, but remain Law Enforcement Sensitive (LES) in order to give SLTLE personnel access.

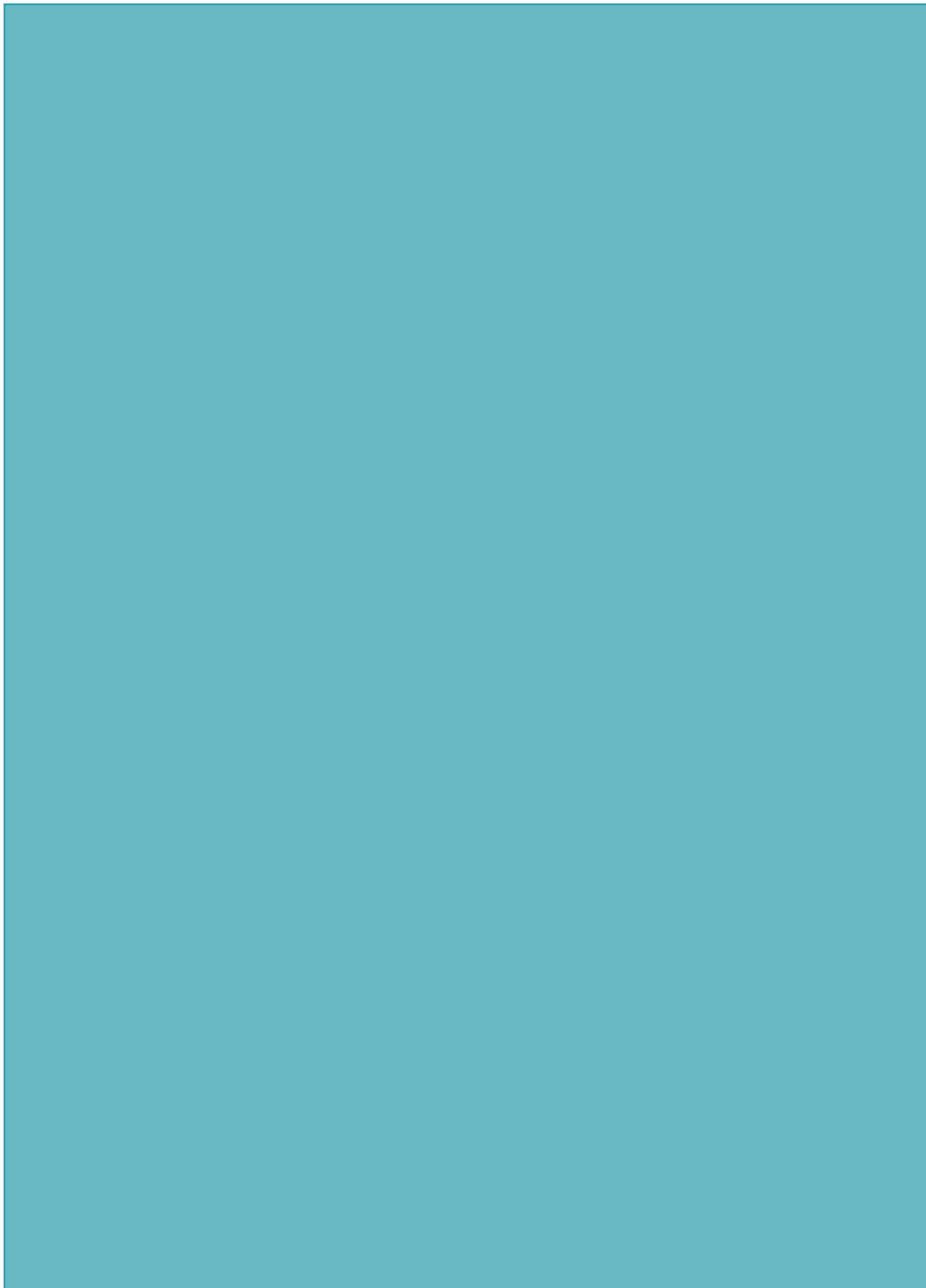
By gaining access to secure networking (e.g., LEO, RISS.net, ATIX, JRIES), interacting on a regular basis with the FBI Field Intelligence Group (FIG), and proactively interacting with other federal law enforcement intelligence offices, SLTLE can have access to the types of critical intelligence necessary to protect their communities.

Summary, Conclusions, and Next Steps

12



CHAPTER TWELVE



Summary, Conclusions, and Next Steps

Effective law enforcement intelligence operations are confusing, controversial, difficult, and effective. Intelligence is confusing because many people do not make the distinction between law enforcement intelligence and national security intelligence. Moreover, the term is used generically to describe a wide body of activities, thereby contributing to the confusion. One purpose of this guide was to provide consistent and clear definitions that are accepted by both law enforcement intelligence professionals and the national standards of the National Criminal Intelligence Sharing Plan, Global Justice Information Sharing Initiative, and the Global Intelligence Working Group.

Law enforcement intelligence operations are controversial both because of the checkered history of intelligence activities as well as the concern of many today that in the zeal to prevent terrorism, citizens' civil rights will be abridged. There is no doubt that law enforcement suffered some setbacks as a result of lawsuits against law enforcement intelligence practices of the 1950s and 1960s. However, with those setbacks important lessons were learned that not only set the stage for 28 CFR Part 23, but helped lay the foundation for law enforcement intelligence as a profession today.

Further controversies face law enforcement today as concerned citizens and civil rights groups, who often do not fully understand the intelligence function, fear that law enforcement agencies will gather and keep information about citizens who have not committed crimes but are exercising their civil rights on controversial issues. The lessons law enforcement has learned from public education and community policing initiatives can help eliminate these fears—not only through the practice of ethical policing²⁰⁹ but also by reaching out to diverse communities to explain police practices, respond to questions, and establishing open, trusted lines of communication.²¹⁰

Intelligence operations are difficult as well. It requires work to establish links with different law enforcement organizations and groups to maximize effective information sharing. It also requires a redistribution of resources to make the intelligence function perform effectively and to meet operational and training standards set out in the National Criminal Intelligence Sharing Plan. A change in culture is required for Intelligence-Led Policing to become a reality and a realignment of priorities may be needed to accomplish new goals. There is always resistance to change and always legitimate competing interests that must be weighed.

Finally, law enforcement intelligence processes can be effective. Intelligence can help identify suspected criminals, targets of terrorists, and activities of criminal enterprises that occur in a community. It takes diverse and often disparate information, integrates it into a cohesive package, and provides insight that might otherwise be lost. Increasingly, law enforcement intelligence is more thorough, of higher quality, and disseminated more broadly as a result of cooperative initiatives such as the

209 The COPS Regional Community Policing Institutes RCPI have a variety of training curricula for executives and line officers on different aspects of ethical policing. Agencies should contact the RCPI in their region for training opportunities. RCPIs can be found by state at: <http://www.cops.usdoj.gov/default.asp?Item=229>.

210 The COPS Office sponsored an executive session with the Police Executive Research Forum that examined this topic. The resulting white paper, *Working with Diverse Communities*, is a valuable resource. It can be found at: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1364>.

National Criminal Intelligence Sharing Plan and the Global Justice Information Sharing Initiative, particularly through its subcommittee, the Global Intelligence Working Group. Similarly, there is a greater emphasis on law enforcement intelligence and a renewed spirit of partnership between the FBI and state, local, and tribal law enforcement (SLTLE) agencies that is already bearing fruit. The end result of all of these initiatives is to make our communities safer; hence, the investment pays important dividends for protecting our citizens.

Similarly, there is a greater emphasis on law enforcement INTELLIGENCE and a renewed SPIRIT of partnership between the FBI and state, local, and tribal law enforcement (SLTLE) agencies that is already bearing fruit.

IMPLEMENTING CHANGE: THE R-CUBED APPROACH²¹¹

Implementing new intelligence initiatives can be difficult. As a road map to accomplish this, the author recommends a process referred to as “R-cubed”: Reassessing, Refocusing, and Reallocating (R3).

211 Carter, David L. (2000). *The Police and Community*. 7th ed. Upper Saddle River, NJ: Prentice-Hall.

The intent of the R3 exercise is to provide a framework for organizational change as related to intelligence responsibilities. It requires a critical self-assessment of responsibilities and resources; objectivity absent special interests; realistic perspectives; both tactical and strategic considerations of traditional and new policing responsibilities; and methods (including financing) of how all police responsibilities will be accomplished. This is a labor-intensive, difficult process that cannot be rushed and should be inclusive, that is, consideration of the inputs of others—employees, community members, elected officials, other agencies—should be included in the process. Final decisions, however, remain with law enforcement administrators to make changes as best determined by their collective judgment of responsibilities, priorities, and available resources.

A number of factors may be included in each component of the R3 exercise, as described below.

Reassessing

Examine both current priorities and new priorities for intelligence and homeland security to determine what activities need to be continued to maintain community safety and fulfill the police mission related to crime, order maintenance, and terrorism. This assessment should include consideration of a number of variables, such as the following:

- The number of calls for service received by the police department and the ability to handle those calls for service.
- Specialization currently in the police department, e.g., gangs, narcotics, school programs, initiatives directed toward senior citizens, traffic, etc., and the true demand or need for that specialization
 - Objectivity is critical because special interests can skew priorities
- Specialization that needs to be developed, e.g., intelligence capacity; first responder (including weapons of mass destruction); computer crime/cyberterrorism prevention and investigative expertise; investigative capacity for terrorism; obligation to assign personnel to the Joint Terrorism Task Force
- Resources that can be used to help with police responsibilities of all forms, e.g., police reserves, volunteers, expertise in other agencies, community organizations
- Objective assessment of threats and potential targets within the community and within the region (the latter includes how multijurisdictional crime and terrorist threats would affect an agency directly and indirectly, including mutual aid obligations)
- Current intelligence expertise and practices, including information sharing, and the need to modify these practices, including adding a private sector component for critical infrastructure.
- Political mandates from elected officials and/or the community that should not be ignored because expectations and concerns of these groups must be taken into account in any assessment process.

Refocusing

Guided by the results of the reassessment, a department must develop a plan incorporating its new priorities, as appropriate. Virtually all of the department's current tasks will continue in some form, but the amount of emphasis and proportion of resources devoted to those tasks will differ, notably in light of added homeland security needs.

Refocusing first requires the department to establish its new priorities by reassessing and evaluating its responsibilities. From there it can refocus on its priorities, if needed. *Reassessment* involves information gathering and analysis. *Refocusing* is implementing policy steps to make the changes operational.

Second, each area of responsibility must be weighted (i.e., weight constitutes the amount of emphasis given to each broad area of tasks and determines which area receives the greatest amount of attention.) The author does not suggest that intelligence should be the top priority; indeed, in most police agencies managing calls for service will remain the top priority. Instead, this is a realistic expectation that priorities will change with the addition of intelligence/homeland security and that all responsibilities will be affected to some degree. Therefore, to determine this realignment, responsibilities and weights must be stipulated.

Third, these changes are actually implemented through the issuance of updated (and new when applicable) policies, procedures, and orders. Implementation also requires communication and, in some cases, in-service training to explain and clarify the changes.

Reallocating

Once refocusing decisions have been made, the department must reallocate its resources to meet adjusted priorities. This includes personnel, operating expenses, equipment (from cars to radios to computers), and office space, as needed. There is always the possibility

that the department will receive an increased appropriation for homeland security in its budget. If so, most likely it will be only a proportion of actual resource needs. The difficult process of reallocation is a necessity that will produce some alienation and, in all likelihood, political rifts within the organization. Reallocation, therefore, also requires effective leadership to guide the organization and motivate personnel to understand the necessity of the changes and the concomitant benefits to the community.

There is no explicit recipe for change in an organization. This is particularly true with intelligence where a renewed emphasis is given to a process that is largely not understood by most personnel. There is little guidance and, despite the best plans, time will be needed for experimentation. Agencies should take the time to carefully consider all new responsibilities, balance them with legitimate competing demands within the agency, and make a clear step toward adjusting the organization.

CONCLUSION

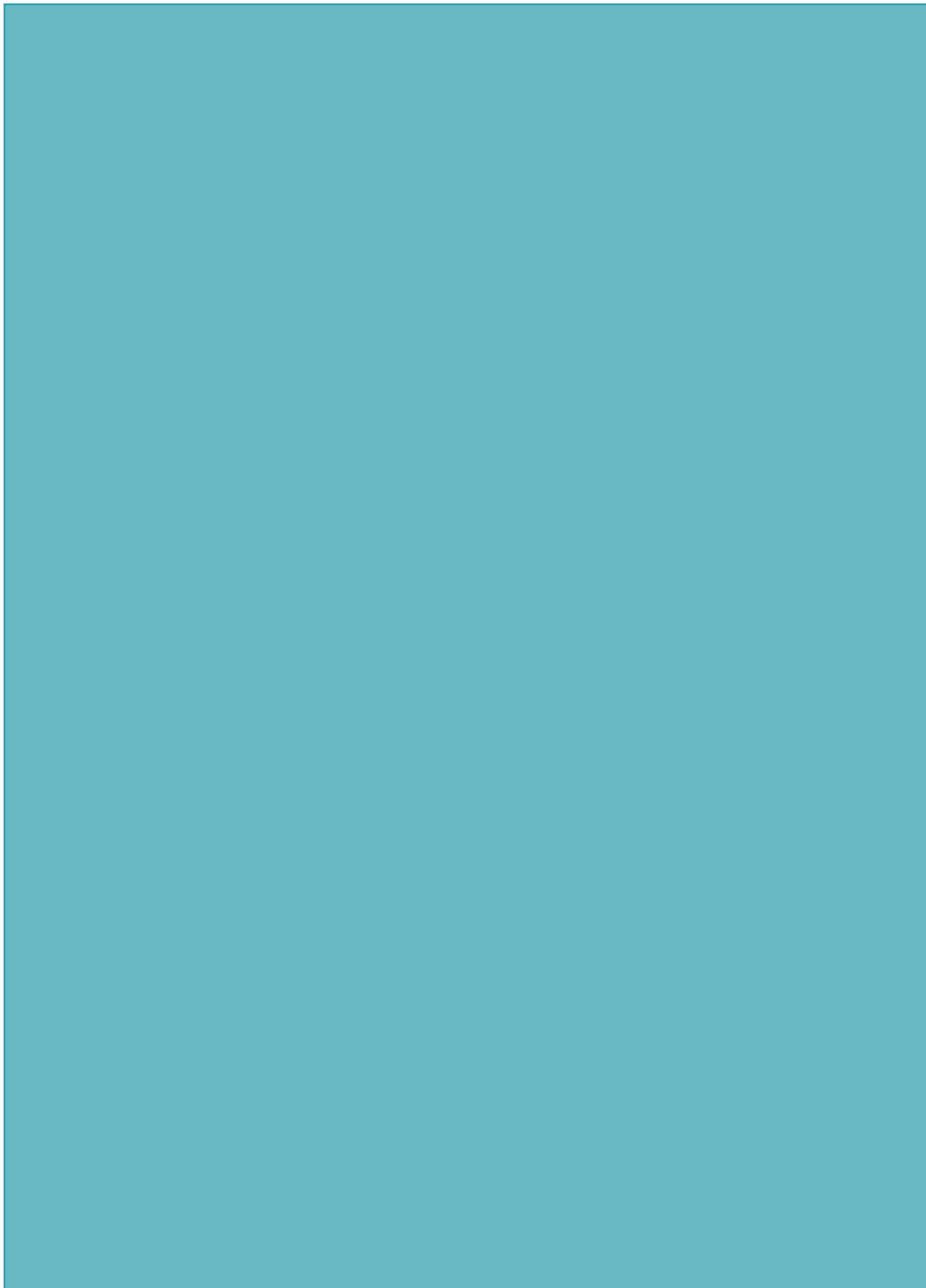
As demonstrated throughout this guide, America's law enforcement agencies are facing a new challenge. Throughout the history of policing challenges have been faced, they have been met with resolute determination, and America has been safer as a result. This new challenge is no different. The intent of this guide has been to help America's state, local, and tribal law enforcement agencies make this journey.

Throughout the history of POLICING CHALLENGES have been faced, they have been met with RESOLUTE DETERMINATION, and AMERICA has BEEN SAFER as a result.

Appendices



APPENDIX A

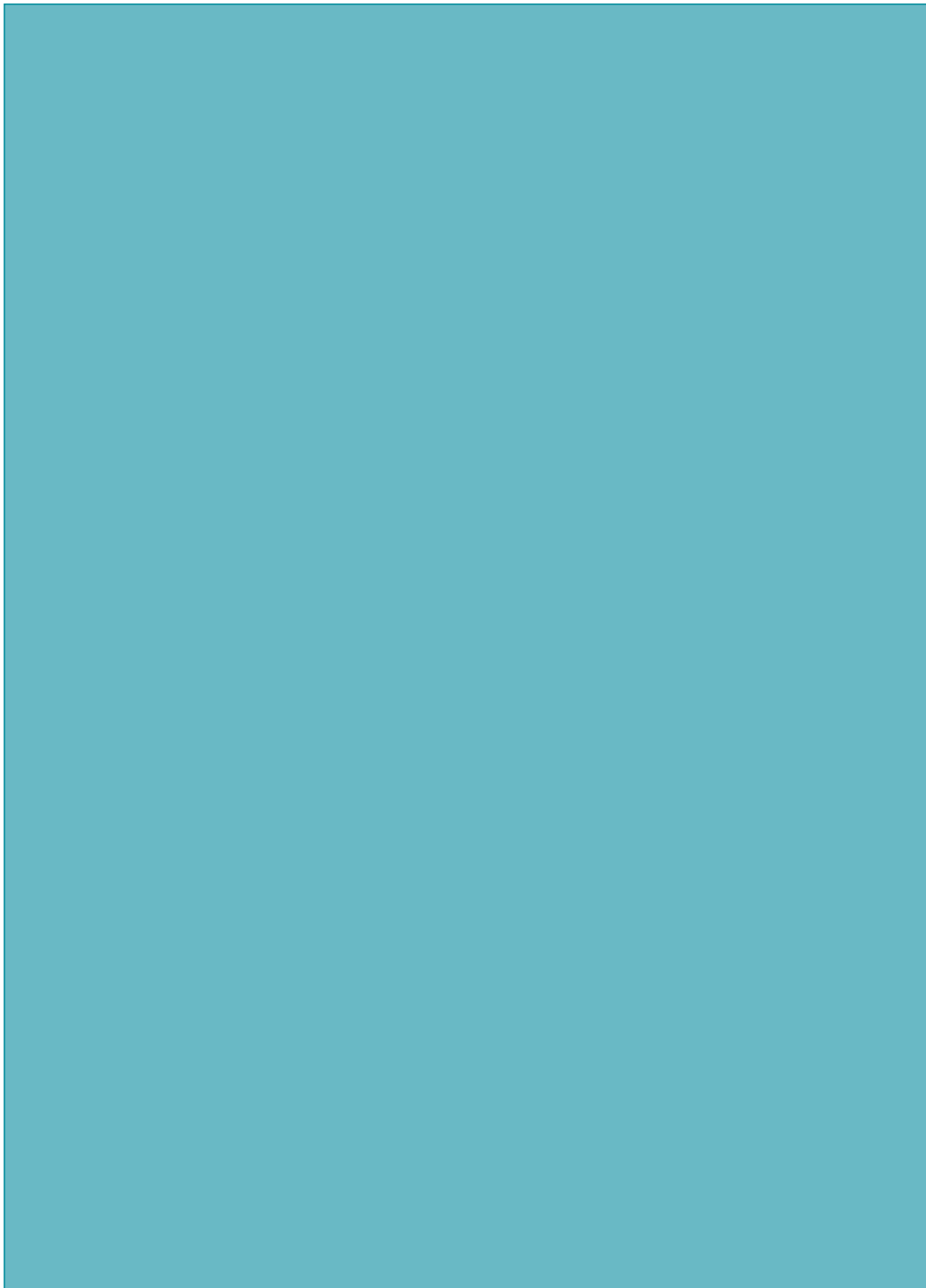


Advisory Board

Advisory Board Members

<p>Doug Bodrero President and CEO Institute for Intergovernmental Research Post Office Box 12729 Tallahassee, FL 32317-2729</p>	<p>Theron Bowman, Ph.D. Chief Arlington, Texas Police Department 620 West Division Street Arlington, TX 76011</p>
<p>Michael A. Braun Acting Assistant Administrator Intelligence Drug Enforcement Administration 700 Army-Navy Drive Arlington, VA 22202</p>	<p>Melvin J. Carraway Superintendent Indiana State Police IGCN - 100 North Senate Avenue Indianapolis, IN 46204-2259</p>
<p>Robert Casey, Jr. Deputy Assistant Director Office of Intelligence, FBI Headquarters 935 Pennsylvania Avenue, NW Washington, DC 20535</p>	<p>Eileen Garry Deputy Director Bureau of Justice Assistance U.S. Department of Justice 810 Seventh Street, NW Washington, DC 20531</p>
<p>Ellen Hanson Chief Lenexa Police Department 12500 W. 87th St. Parkway Lenexa, KS 66215</p>	<p>Gil Kerlikowske Chief Seattle Police Department 610 Fifth Avenue Seattle, WA 98124-4986</p>
<p>William Mizner Chief Norfolk Police Department 202 N. 7th Street Norfolk, NE 68701</p>	<p>William Parrish Senior Representative Dept. of Homeland Security, Liaison Office FBI HQ Room 5885 935 Pennsylvania Avenue, NW Washington, DC 20535</p>
<p>Theodore Quasula Chief Law Enforcement Officer Las Vegas Paiute Tribe Police 1 Paiute Drive Las Vegas, NV 89106</p>	<p>Darrel Stephens Chief Charlotte-Mecklenburg Police Department 601 East Trade Street Charlotte, NC 28202</p>
<p>Bill Young Sheriff Las Vegas Metropolitan Police Department 400 Stewart Avenue Las Vegas, NV 89101-2984</p>	

APPENDIX B



Law Enforcement
Intelligence Unit (LEIU)
Criminal Intelligence File Guidelines ²¹²

I. CRIMINAL INTELLIGENCE FILE GUIDELINES

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

II. CRIMINAL INTELLIGENCE FILE DEFINED

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
2. Are suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
2. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

III. FILE CONTENT

Only information with a criminal predicate and which meets the agency's criteria for file input should be stored in the criminal intelligence file.

Specifically excluded material includes:

- A. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.
- B. Information on an individual or group merely on the basis of ethnic background.
- C. Information on any individual or group merely on the basis of religious or political affiliations.
- D. Information on an individual or group merely on the basis of non-criminal personal habits.
- E. Criminal Offender Record Information (CORI), should be excluded from an intelligence file. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy.
- F. Also excluded are associations with individuals that are not of a criminal nature.

State law or local regulations may dictate whether or not public record and intelligence information should be kept in separate files or commingled. Some agencies believe that separating their files will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded, as all information requested in the subpoena (both public and intelligence) must be turned over to the court. The judge then makes the determination on what information will be released.

The decision to commingle or separate public and intelligence documents is strictly a management decision. In determining this policy, administrators should consider the following:

- A. Records relating to the conduct of the public's business that are prepared by a state or local agency, regardless of physical form or characteristics, may be considered public and the public has access to these records.

- B. Specific types of records (including intelligence information) may be exempt from public disclosure.
- C. Regardless of whether public record information is separated from or commingled with intelligence data, the public may have access to public records.
- D. The separation of public information from criminal intelligence information may better protect the confidentiality of the criminal file. If a request is made for public records, an agency can release the public file and leave the intelligence file intact (thus less apt to accidentally disclose intelligence information).
- E. Separating of files is the best theoretical approach to maintaining files; however, it is not easy to do. Most intelligence reports either reference public record information or else contain a combination of intelligence and public record data. Thus, it is difficult to isolate them from each other. Maintaining separate public and intelligence files also increases the amount of effort required to index, store, and retrieve information.

IV. FILE CRITERIA

All information retained in the criminal intelligence file should meet file criteria prescribed by the agency. These criteria should outline the agency's crime categories and provide specifics for determining whether subjects involved in these crimes are suitable for file inclusion.

File input criteria will vary among agencies because of differences in size, functions, resources, geographical location, crime problems, etc. The categories listed in the suggested model below are not exhaustive.

- A. Permanent Status
 - 1. Information that relates an individual, organization, business, or group is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

- Narcotic trafficking/manufacturing
 - Unlawful gambling
 - Loan sharking
 - Extortion
 - Vice and pornography
 - Infiltration of legitimate business for illegitimate purposes
 - Stolen securities
 - Bribery
 - Major crime including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson
 - Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation
 - Threats to public officials and private citizens.
2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable—distinguished by a name and unique identifying characteristics (e.g., date of birth, criminal identification number, driver's license number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. NOTE: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.

B. Temporary Status:

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given “temporary” status. It is recommended the retention of temporary information not exceed 1 year unless a compelling reason exists to extend this time period. (An example of a compelling reason is if

several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified temporary at the end of the 1 year period, and a compelling reason for its retention is not evident, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1. Subject/entity is unidentifiable – subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.
2. Involvement is questionable – involvement in criminal activities is suspected by a subject/entity which has either:
 - Possible criminal associations – individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.
 - Criminal history – individual, organization, business, or group (not currently reported to be criminally active) that has a history of criminal conduct, and the circumstances currently being reported (i.e., new position or ownership in a business) indicates they may again become criminally active.
3. Reliability/validity unknown – the reliability of the information sources and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

V. INFORMATION EVALUATION

Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing. The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness.

Circulating information which may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy.

To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

Source Reliability:

- (A) Reliable – The reliability of the source is unquestioned or has been well tested in the past.
- (B) Usually Reliable – The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
- (C) Unreliable – The reliability of the source has been sporadic in the past.
- (D) Unknown – The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity:

- (1) Confirmed – The information has been corroborated by an investigator or another independent, reliable source.

- (2) Probable – The information is consistent with past accounts.
- (3) Doubtful – The information is inconsistent with past accounts.
- (4) Cannot Be Judged – The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of the information to persons outside the agency. However, the classification of information in itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

Classification systems may differ among agencies as to the number of levels of security and release authority. In establishing a classification system, agencies should define the types of information for each security level, dissemination criteria, and release authority. The system listed below classifies data maintained in the Criminal Intelligence File according to one of the following categories:

Sensitive

1. Information pertaining to significant law enforcement cases currently under investigation.

2. Corruption (police or other government officials), or other sensitive information.
3. Informant identification information.
4. Criminal intelligence reports which require strict dissemination and release criteria.

Confidential

1. Criminal intelligence reports not designated as sensitive.
2. Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Restricted

1. Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists.
2. Nonconfidential information prepared for/by law enforcement agencies.

Unclassified

1. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).
2. News media information – newspaper, magazine, and periodical clippings dealing with specified criminal categories.

VII. INFORMATION SOURCE

In all cases, source identification should be available in some form. The true identity of the source should be used unless there is a need to protect the source. Accordingly, each law enforcement agency should establish

criteria that would indicate when source identification would be appropriate.

The value of information stored in a criminal intelligence file is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

- The nature of the information reported.
- The potential need to refer to the source's identity for further or prosecutorial activity.
- The reliability of the source.

Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases when identifying the source by name is not practical for internal security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the intelligence unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information (for example "S- 60, a reliable police informant heard" or "a reliable law enforcement source of the police department saw" a particular event at a particular time).

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence files conforms with the agency's file criteria and has been properly evaluated and classified.

IX. FILE DISSEMINATION

Agencies should adopt sound procedures for disseminating stored information. These procedures will protect the individual's right to privacy as well as maintain the confidentiality of the sources and the file itself.

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a “need-to-know” and a “right-to-know.”

“Right-to-know” Requestor has official capacity and statutory authority to the information being sought.

“Need-to-know” Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No “original document” which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

Information classification and evaluation are, in part, dissemination controls. They denote who may receive the information as well as the internal approval level(s) required for release of the information. In order to encourage conformity within the intelligence community, it is recommended that stored information be classified according to a system similar to the following.

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. To eliminate unauthorized use and abuses of the system, a department should utilize a dissemination control form that could be maintained with each stored document. This control form would record the date of the request, the name of the agency and individual requesting the information, the need-to-know, the information provided, and the name of the employee handling the request. Depending upon the needs of the agency, the control form also may be designed to record other items useful to the agency in the management of its operations. This control form also may be subject to discovery.

Security Level	Dissemination Criteria	Release Authority
Sensitive	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Intelligence Unit Commander
Confidential	Same as for Sensitive	Intelligence Unit Manager or Designee
Restricted	Same as for Sensitive	Intelligence Unit Supervisor or Designee
Unclassified	Not Restricted	Intelligence Unit Personnel

X. FILE REVIEW AND PURGE

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to: ensure that the file is current, accurate, and relevant to the needs and objective of the agency; safeguard the individual's right of privacy as guaranteed under federal and state laws; and, ensure that the security classification level remains appropriate.

Law enforcement agencies have an obligation to keep stored information on subjects current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge criteria and schedules. Operational procedures for the purge and the method of destruction for purged materials should be established.

A. Purge Criteria:

General considerations for reviewing and purging of information stored in the criminal intelligence file are as follows:

1. Utility

- How often is the information used?
- For what purpose is the information being used?
- Who uses the information?

2. Timeliness and Appropriateness

- Is this investigation still ongoing?
- Is the information outdated?
- Is the information relevant to the needs and objectives of the agency?
- Is the information relevant to the purpose for which it was collected and stored?

3. Accuracy and Completeness

Is the information still valid?

Is the information adequate for identification purposes?

Can the validity of the data be determined through investigative techniques?

B. Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every 5 years for permanent documents. Agencies should develop a schedule best suited to their needs and should contact their legal counsel for guidance.

C. Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. Disposal is used for all records or papers that identify a person by name. It is the responsibility of each agency to determine that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

XI. FILE SECURITY

The criminal intelligence file should be located in a secured area with file access restricted to authorized personnel.

Physical security of the criminal intelligence file is imperative to maintain the confidentiality of the information stored in the file and to ensure the protection of the individual's right to privacy.

GLOSSARY

Public Record

Public record includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

"Member of the public" means any person, except a member, agent, officer, or employee of a federal, state, or local agency acting within the scope of his or her membership in an agency, office, or employment.

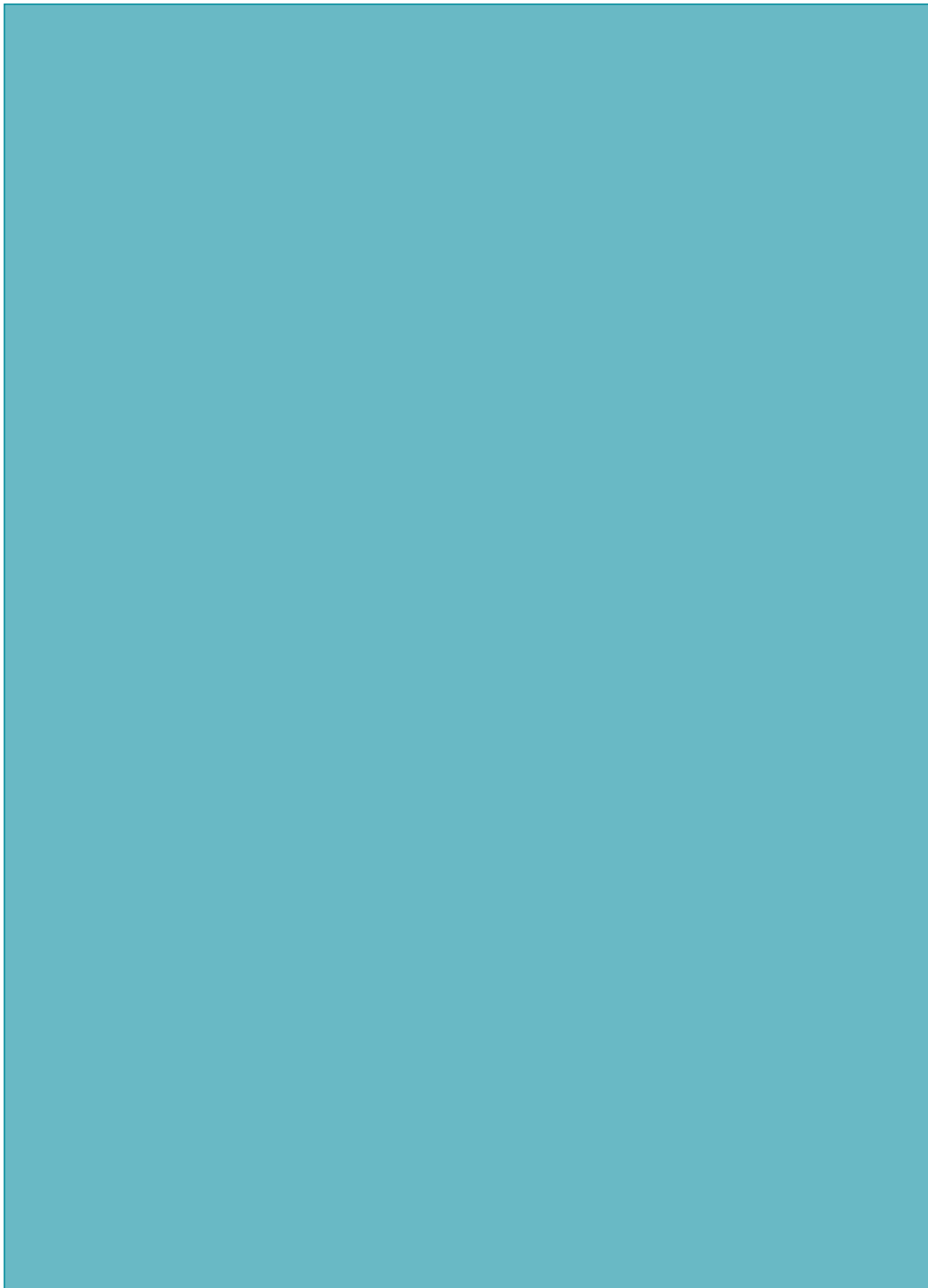
For purposes of these guidelines, public record information includes only that information to which the general public normally has direct access, (i.e., birth or death certificates, county recorder's information, incorporation information, etc.)

Criminal Offender Record Information (CORI)

CORI is defined as summary information to arrests, pretrial proceedings, sentencing information, incarcerations, parole, and probation.

- a. Summary criminal history records are commonly referred to as “rap sheets.” Data submitted on fingerprint cards, disposition of arrest and citation forms and probation flash notices create the entries on the rap sheet.

APPENDIX C



Intelligence Unit Management Audit

Audit Factors for the Law Enforcement Intelligence Function²¹³

213 Prepared by David L. Carter, Michigan State University, for an audit of the Denver, Colorado Police Department Intelligence Bureau in compliance with a U.S. District Court settlement. Copyright © 2004 by David L. Carter. All rights reserved.

214 http://it.ojp.gov/topic.jsp?topic_id=8

215 http://it.ojp.gov/topic.jsp?topic_id=93

216 <http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf>

217 http://www.calea.org/newweb/accreditation%20Info/descriptions_of_standards_approv.htm

218 http://it.ojp.gov/process_links.jsp?link_id=3774

219 http://it.ojp.gov/process_links.jsp?link_id=3773

220 http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_type_id=1&document_id=95

221 http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_type_id=1&document_id=94

222 As one good example, see the Santa Clara, CA Police Department's Value Statements at http://www.scpd.org/value_statement.html.

223 <http://www.iir.com/28cfr/>

Section A. Meeting National Standards

1. Does the police department subscribe to the tenets and standards of the *Global Justice Information Sharing Initiative*?²¹⁴
☐ Yes ☐ No
2. Does the police department subscribe to the standards of the *National Criminal Intelligence Sharing Plan*?²¹⁵
☐ Yes ☐ No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the Office of Domestic Preparedness *Guidelines for Homeland Security*?²¹⁶
☐ Yes ☐ No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 *Criminal Intelligence*?²¹⁷
☐ Yes ☐ No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) *Model Criminal Intelligence Policy*?²¹⁸
☐ Yes ☐ No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines*?²¹⁹
☐ Yes ☐ No
7. Does the police department subscribe to the IACP *Code of Ethics* ²²⁰ or have an articulated Code of Ethics?
☐ Yes ☐ No
8. Does the police department subscribe to the IACP *Code of Conduct* ²²¹ or have an articulated Code of Conduct?
☐ Yes ☐ No
9. Does the police department have an articulated Statement of Values?²²²
☐ Yes ☐ No
10. Does the police department adhere to the regulations of 28 CFR Part 23²²³ for its Criminal Intelligence Records System?
☐ Yes ☐ No

- a. Does the police department operate a federally funded multi-jurisdictional criminal intelligence records system?
☐ Yes ☐ No
11. Does the police department subscribe to the tenets of the *Justice Information Privacy Guidelines*?²²⁴
☐ Yes ☐ No
12. Does the police department subscribe to the tenets for information system security defined in the report, *Applying Security Practices to Justice Information Sharing*?²²⁵
☐ Yes ☐ No
13. Does the law enforcement agency subscribe to the philosophy of *Intelligence-Led Policing*?²²⁶
☐ Yes ☐ No
14. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious or doctrinal purpose?
☐ Yes ☐ No

224 <http://www.ncja.org/pdf/privacyguideline.pdf>

225 <http://it.ojp.gov/documents/asp/>

226 <http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport%2Epdf>

227 E.g., collection, analysis, collation, dissemination, contact point for other agencies, clearinghouse, etc.

Section B: Management Issues

1. Has a mission statement been written for the Intelligence Unit?
☐ Yes ☐ No
2. Is the purpose and role of the Unit clearly articulated and related to the Police Department's Mission Statement?
☐ Yes ☐ No
3. Have priorities been established for the types of crimes the Unit will address?
☐ Yes ☐ No
 - a. Is any written rationale provided for these priorities?
☐ Yes ☐ No
4. Are expected activities of the unit articulated?²²⁷
☐ Yes ☐ No
5. Does the mission statement express ethical standards?
☐ Yes ☐ No
6. Does the mission statement express the importance of protecting citizens' rights?
☐ Yes ☐ No

228 The questions in this audit outline the parameters of 28 CFR Part 23 as of the date of this writing. This guideline specifies standards that are required for state and local law enforcement agencies that are operating a federally funded multijurisdictional criminal intelligence system. While the guideline does not apply to all state and local Intelligence Records Systems, the law enforcement intelligence community considers it good practice that all law enforcement agencies should adhere to the standards regardless of whether or not it is formally applicable.

1. Policies and Procedures

1. Are there written and officially articulated policies and procedures for management of the intelligence function?

☐ Yes ☐ No

2. Have intelligence policies been formed to minimize the discretion of information collectors?

☐ Yes ☐ No

If Yes, Describe:

3. Is there a policy and procedures on "Information Collection"?

☐ Yes ☐ No

If Yes, Describe:

2. Management of Information:²²⁸ Definitional Standards (see chart on next page)

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?

☐ Yes ☐ No

2. What is the source of the definitions?

☐ NCISP ☐ Federal Agency

☐ Mixed ☐ N/A

3. Has the department articulated standards for classifying information in the Intelligence Unit?

☐ Yes ☐ No

Priority	Classification	Description	Release Authority
Highest Level	Sensitive	Current corruption case; complex criminality; confidential informants	Dept Executive or Intelligence Cmdr.
Medium Level	Confidential	Non-sensitive information through intelligence channels; Law Enforcement only	Intelligence Unit Cmdr or Supervisor
Lowest Level	Restricted	LE use but no need for high security	Intell Unit Personnel
Unclassified	Public Access	Information that may be released to public and media	Intell Unit Personnel

4. How are those standards monitored and enforced?
☐ Supervisor ☐ Other
5. Does the department have a system for assessing the reliability of sources that provide information that will be retained in the Intelligence Records System?
☐ Yes ☐ No
6. Are there standardized definitions of the reliability scale?
☐ Yes ☐ No
7. Does the department have a system for assessing the validity of the information that will be retained in the Intelligence Records System?
☐ Yes ☐ No
8. Are there standardized definitions of the validity scale?
☐ Yes ☐ No
9. Does the Intelligence Unit have operational definitions that can be applied to a person under investigation or a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a "permanent file" or a "temporary file"?
☐ Yes ☐ No
 If Yes...
 - a. Are the types of identifying information that should be placed in the file articulated?
☐ Yes ☐ No
 - b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?
☐ Yes ☐ No

4. Management of Information: Data Entry

1. Who is responsible for entering information into the Intelligence Records System?
Position/Classification:

2. Who supervises the information entry process?
Position/Classification:

5. Management of Information: Accountability

1. Who is the Custodian of the Intelligence Records System that ensures all regulations, law, policy and procedures are being followed?
Position/Classification:
2. Is there a person external to the Intelligence Unit who is designated to monitor the Intelligence Records System and related processes?
☐ Yes ☐ No
If Yes, Position/Classification):

3. Does the department have written procedures for the retention of records in the Intelligence Records System?
☐ Yes ☐ No

6. Management of Information: Retention and Purging of Records

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?
☐ Yes ☐ No
2. Does the retention policy and procedure include written criteria for purging information?
☐ Yes ☐ No

3. How often does a review and purge process occur?
Frequency:
4. What is the purge process?
Describe:
5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy and relevancy?
☐ Yes ☐ No
6. Does the purge process require destruction of the source document and removal of all references to the document to be purged if the information is no longer appropriate for retention?
☐ Yes ☐ No
7. What is the destruction process for purged "hard copy" records?
Describe:
8. After information has been purged from a computerized Intelligence Records System, is free space on the hard drive and/or specific purged files electronically "wiped"?
☐ Yes ☐ No
- a. Are back-ups wiped?
☐ Yes ☐ No

- b. What is the accountability system for purging back-ups?
Describe:
9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?
☐ Yes ☐ No
10. What is the process for purging partial information from “hard copy” source documents?
Describe:
11. Who is responsible for ensuring compliance of the purge process?
Position/Classification:

7. Management of Information: Personal/Individually-Held Records and Files

1. Is there an intelligence unit policy and procedures concerning the retention of individual notes and records that identifies persons wherein criminality is suspected but is not in either a temporary or permanent file and is not entered into any formal records system or database?
☐ Yes ☐ No

a. How is the possession of personal records monitored?

☐ Yes ☐ No

b. How is the policy enforced?

☐ Yes ☐ No

8. Management of Information: Accessing Intelligence Records

1. Is access to the Intelligence Records limited?

☐ Yes ☐ No

2. If yes, who may access the Intelligence Records System?

Describe:

3. What security controls exist for accessing computerized records?

Describe:

4. Can the computerized records system be accessed through remote access?

☐ Yes ☐ No

a. If so, what security controls exist for remote access?

Describe:

5. How are physical records stored?
Describe:
6. Who grants access privileges to Intelligence Records?
Position/Classification:
7. Who has access to records?
Position/Classification:
8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?
☐ Yes ☐ No
9. What audit process is in place for access to computerized records?
Describe:
10. What audit process is in place for access to physical records?
Describe:

11. How are physical records secured?

Describe:

12. What process is in place to handle unauthorized access to intelligence physical records?

Describe:

13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?

Describe:

9. Physical Location of the Intelligence Unit and Records

1. Sufficiency: Is the Intelligence Unit in a physical location that has sufficient space to perform all of its responsibilities?

☐ Yes ☐ No

2. Security: Is the Intelligence Unit in a physical location wherein the entire workspace may be completely secured?

☐ Yes ☐ No

- a. Is there adequate secured storage cabinets (or a vault) for (1) documents classified by the Intelligence Unit and (2) sensitive records storage within the Intelligence Unit's physical location?
☐ Yes ☐ No
- b. Is there adequate security and segregated storage for federally classified documents within the Intelligence Unit?
☐ Yes ☐ No
- 1) Is that storage accessible only by persons with a federal top secret security clearance?
☐ Yes ☐ No
3. Convenience: Is the Intelligence Unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?
☐ Yes ☐ No

10. Tangential Policy Issues: Criminal Informants and Undercover Operations²³⁰

1. Is there a formally articulated policy and procedures for managing criminal informants?
☐ Yes ☐ No
 - a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?
☐ Yes ☐ No
 - b. Are informant files secured separately from intelligence files?
☐ Yes ☐ No
2. Is there a formally articulated policy and procedures concerning undercover operations that apply to members of the Intelligence Unit?
☐ Yes ☐ No
3. Does the police department have a policy on alcohol consumption for officers working undercover?
☐ Yes ☐ No
 - a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?
☐ Yes ☐ No

230 The use of criminal informants and undercover operations varies between law enforcement agencies. In some cases these resources may be a functional part of the Intelligence Unit, in other cases they are relied on by the unit for information collection. Understanding the management and control of these activities can be important for the intelligence commander for they can reflect the validity, reliability, and constitutional admissibility of the information collected.

4. Does the police department have a “narcotics simulation” policy and training for undercover officers?
☐ Yes ☐ No
5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?
☐ Yes ☐ No
6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?
☐ Yes ☐ No
7. With respect to undercover operating funds:
 - a. Is there a 1-tier or 2-tier process to approve use of the funds?
☐ 1 Tier ☐ 2 Tier
 - b. Is a written report required to document expenditure of the funds?
☐ Yes ☐ No
 - c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?
Days ☐ No Set Time
 - d. Is there a regular external audit of undercover funds?
☐ Yes [How Often?] ☐ No

Section C: Personnel

1. Is a position classification plan in place that provides a clear job description for each position in the unit?
☐ Yes ☐ No
2. Is a position classification plan in place that articulates Knowledge, Skills and Abilities (KSAs) for each position?
☐ Yes ☐ No
3. Is there sufficient hierarchical staff (managers/supervisors) assigned to the unit to effectively perform supervisory responsibilities?
☐ Yes ☐ No
4. Is there sufficient functional staff (analysts and/or investigators) to effectively fulfill defined unit responsibilities?
☐ Yes ☐ No

5. Is there sufficient support staff (secretaries, clerks) to effectively support the unit's activities?
☐ Yes ☐ No
6. Does the screening process for nonsworn employees of the intelligence unit require:
- a. Fingerprint check?
☐ Yes ☐ No
- b. Background investigation
☐ Yes ☐ No
7. If the Intelligence Unit has non-PD employees assigned to it – e.g., National Guard analysts, personnel from the state or local law enforcement agencies – would there be a screening process for those persons?
☐ Yes ☐ No
- If Yes, Describe:

1. Training

1. What types of training do preservice and newly assigned personnel receive?
☐ None ☐ Some–Describe:
- a. Are newly assigned sworn employees to the Intelligence Unit required to attend 28 CFR Part 23 training?
☐ Yes ☐ No
- b. Are newly hired or assigned non-sworn employees required to attend 28 CFR Part 23 training?
☐ Yes ☐ No

2. What types of training do in-service personnel receive?²³¹

☐ None ☐ Some

Describe:

3. Have members of the Intelligence Unit attended any of the following federal government intelligence training programs which are open to state and local law enforcement officers?

a. DEA Federal Law Enforcement Analyst Training (FLEAT)?

☐ Yes ☐ No

b. FBI College of Analytic Studies?

☐ Yes ☐ No

c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course?

☐ Yes ☐ No

d. National Drug Intelligence Center Basic Intelligence Analysis Course?

☐ Yes ☐ No

e. National White Collar Crime Center Foundations of Intelligence Analysis?

☐ Yes ☐ No

f. Regional Counterdrug Training Academy Intelligence Operations Course?

☐ Yes ☐ No

²³¹ Note: Training should go beyond "the basics" and include updates of law, current crime issues, and trends; new technologies, new resources, etc.

2. Supervision

1. Does supervision effectively monitor adherence to written procedures?

☐ Yes ☐ No

2. Does supervision effectively monitor adherence to guidelines adopted by the department?

☐ Yes ☐ No

3. Are performance evaluations tied directly to the job descriptions?²³²
☐ Yes ☐ No
4. Does supervision effectively monitor the performance of required duties (Including the quality of performance)?
☐ Yes ☐ No
5. Is supervision effectively monitoring personnel to ensure civil rights allegations cannot be made with respect to negligent:
 - a. Failure to train?
☐ Yes ☐ No
 - b. Hiring?
☐ Yes ☐ No
 - c. Failure to supervise?
☐ Yes ☐ No
 - d. Assignment?
☐ Yes ☐ No
 - e. Failure to direct?
☐ Yes ☐ No
 - f. Failure to discipline?
☐ Yes ☐ No
 - g. Entrustment?
☐ Yes ☐ No
6. Is there effective supervision of the Intelligence Unit throughout the chain of command external to the Intelligence Unit?
☐ Yes ☐ No

232 Intelligence Unit staff responsibilities are sufficiently different from other police positions that standard performance evaluations typically do not apply (particularly those evaluations that have a quantitative component).

Section D: Fiscal Management

1. Is the budget sufficient to fulfill the stated mission?
☐ Yes ☐ No
2. Does the Intelligence Commander have input into the budget planning process?
☐ Yes ☐ No

3. Is there over-reliance on “soft money” to operate the unit?²³³
☐ Yes ☐ No
4. Are equipment and personnel line items assigned directly to the Intelligence Unit?²³⁴
☐ Yes ☐ No
5. Is there an established process for reliably monitoring credit cards assigned to personnel?
☐ Yes ☐ No ☐ NA

Section E: Unit Evaluation

1. As a whole, is the unit effective with respect to:
 - a. Providing information to prevent crime?
☐ Yes ☐ No
 - b. Providing information to apprehend criminals?
☐ Yes ☐ No
 - c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?
☐ Yes ☐ No
2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence unit's productivity as an organizational entity?
 - a. Number and type of analytic products delivered for investigative purposes?
☐ Yes ☐ No ☐ NA
 - b. Number and type of analytic products that led to arrest?
☐ Yes ☐ No ☐ NA
 - c. Assets seized from illegal activities wherein intelligence contributed to the arrest and/or seizure?
☐ Yes ☐ No ☐ NA
 - d. Number and types of strategic intelligence products delivered to the command staff?
☐ Yes ☐ No ☐ NA
 - e. Number of intelligence-sharing meetings attended by unit staff?
☐ Yes ☐ No ☐ NA
 - f. Number of briefings provided by the intelligence staff?
☐ Yes ☐ No ☐ NA

²³³ For example, grants, cooperative agreements, contracts with other agencies, etc.

²³⁴ N.B.: If they are not specifically assigned, then they can be withdrawn more easily.

- g. Total number of queries into the intelligence data base?
☐ Yes ☐ No ☐ NA
 - h. Number of permanent files opened?
☐ Yes ☐ No ☐ NA
 - i. Number of temporary files investigated?
☐ Yes ☐ No ☐ NA
 - j. Number of requests for information to the unit from outside agencies?
☐ Yes ☐ No ☐ NA
3. Are products produced by the Intelligence Unit:
- a. In a consistent format?
☐ Yes ☐ No
 - b. Easily consumed and used (i.e., understandable and actionable)?
☐ Yes ☐ No
 - c. Contain timely information and disseminated in a timely manner?
☐ Yes ☐ No
 - d. Have substantive contact to aid in preventing or controlling crime?
☐ Yes ☐ No
4. Given the confidential nature of the information contained in the Intelligence Unit, is there a policy and procedures if a city, county, state, or federal fiscal or program auditor seeks to audit the Intelligence Unit?
☐ Yes ☐ No
- If Yes, Describe:

Section F. Collection

1. Is there an articulated collection plan for the Intelligence Unit?

☐ Yes ☐ No

If Yes, Describe:

- a. How often and when is the plan updated?

Describe:

2. Have the following activities been performed by the Intelligence Unit:

- a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists?

☐ Yes ☐ No

- b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region?

☐ Yes ☐ No

- c. A target or criminal commodity analysis of the region?

☐ Yes ☐ No

- d. A target or criminal commodity vulnerability assessment in the region?

☐ Yes ☐ No

3. For each identified threat, have intelligence requirements been articulated?

☐ Yes ☐ No

- a. If Yes, Describe the methods of collection that will be used to fulfill those intelligence requirements.

Section G: Technology and Networking

1. Are any members of the Intelligence Unit subscribed members to the FBI's secure Email system Law Enforcement Online (LEO)?
☐ Yes-All ☐ Yes-Some ☐ No
2. Are any members of the Intelligence Unit subscribed members to the secure Regional Information Sharing System (RISS) email system riss.net?
☐ Yes-All ☐ Yes-Some ☐ No
 - a. If yes, are the RISS databases (e.g., RISS.gang, ATIX, etc.) regularly used?
☐ Yes ☐ No
3. Is the police department a member of the Regional Information Sharing System?²³⁵
☐ Yes ☐ No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted via the National Law Enforcement Teletype System (NLETS) are forwarded to the Intelligence Unit?
☐ Yes ☐ No
5. Are you connected to any state-operated intelligence or information networks?
☐ Yes ☐ No
If Yes, Describe:

²³⁵ The six Regional Information Sharing System centers are: MAGLOCLEN, MOCIC, NESPIN, RMIN, ROCIC, WSIN. See http://www.iir.com/riss/RISS_centers.htm.

6. Are you connected to any regional intelligence or information networks (including HIDTA)?

☐ Yes ☐ No

If Yes, Describe:

7. Does the intelligence have access and use the National Virtual Pointer²³⁶ System (NVPS)?²³⁷

☐ Yes ☐ No

8. Is there a formal approval process for entering into a memorandum of understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?

☐ Yes ☐ No

If Yes, Describe the process:

236 A Pointer System – also known as a deconfliction center – determines when two different agencies are investigating the same criminal incident to same person. Since two agencies are investigating the same entity, they are possibly in conflict. In order to “deconflict”, the pointer system notifies both agencies of their mutual interest in a case/person in order to avoid duplication of effort, conflicting approaches, and increasing efficiency and effectiveness.

237 NVPS integrates HIDTA, NDPIX, and RISS pointers via secure web-based communications.

Who must approve the MOU?

Section H: Legal Issues

1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?

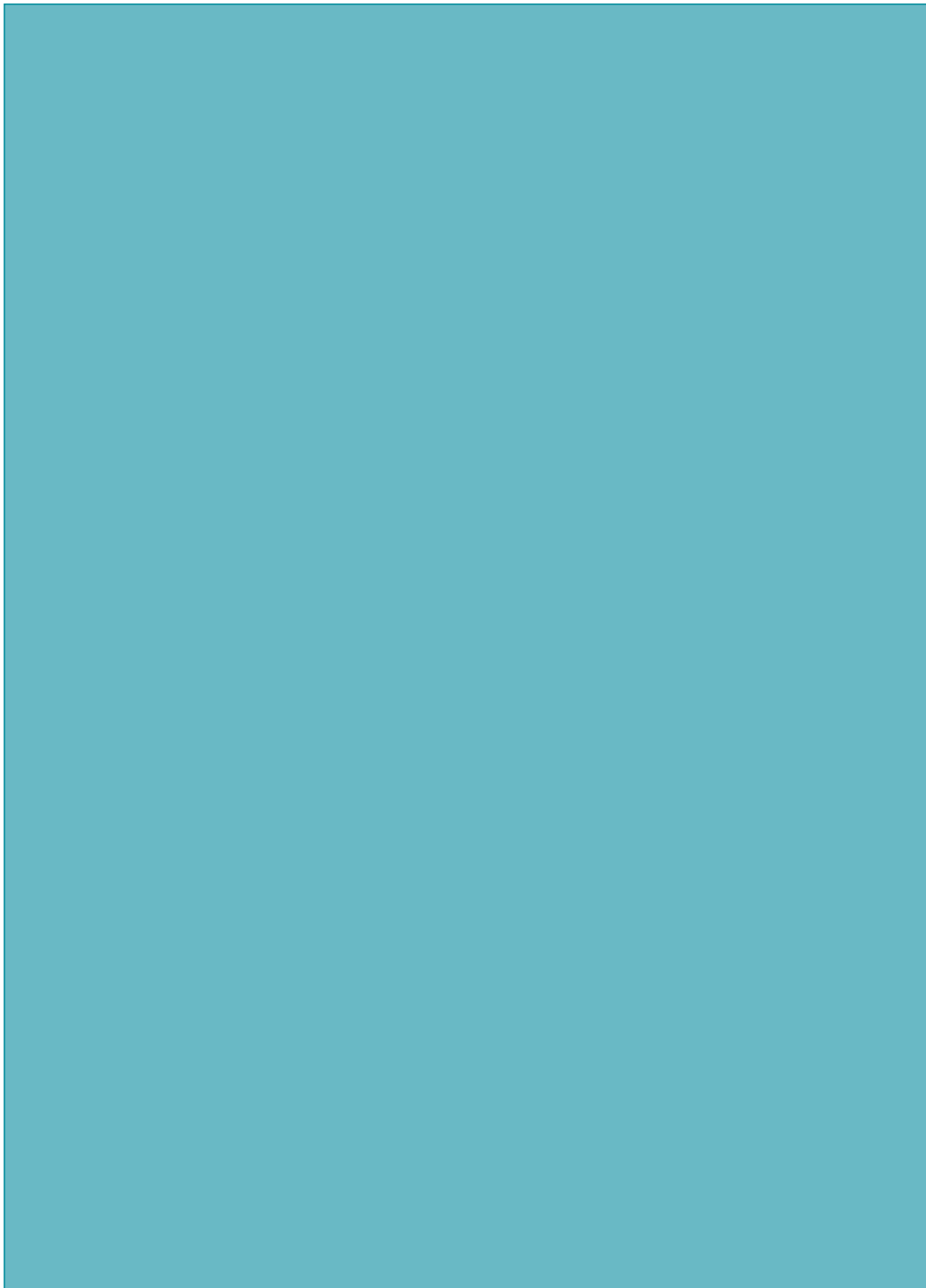
☐ Yes ☐ No

2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the intelligence unit?

☐ Yes ☐ No

3. Is there a designated person the police department contacts in response to a subpoena for a file in the Intelligence Records System?
☐ Yes ☐ No
4. Does the Intelligence Unit Commander have a legal resource for advice to help protect intelligence records from objectionable access?
☐ Yes ☐ No
5. Does the Intelligence Unit Commander have a legal resource for advice on matters related to criminal procedure and civil rights?
☐ Yes ☐ No
6. Does the Intelligence Unit Commander have a legal resource for advice on matters related to questions of civil liability as it relates to all aspects of the intelligence function?
☐ Yes ☐ No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
☐ Yes ☐ No

APPENDIX D



28 CFR Part 23

28 CFR Part 23

Criminal Intelligence Systems Operating Policies²³⁸

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

²³⁸ Based on Executive Order 12291, February 17, 1981. The list of executive orders can be found at the National Archive website: <http://www.archives.gov/>. The most current text of 28 CFR Part 23 can be found at the Library of Congress website by retrieving the regulation from the Code of Federal Regulations (CFR) search engine at: <http://www.gpoaccess.gov/cfr/index.html>.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence information only to law enforcement

authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

- (a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.
- (b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:
 - (1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and
 - (2) Involve a significant degree of permanent criminal organization; or
 - (3) Are not limited to one jurisdiction.
- (c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.
- (d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

28 CFR Part 23: 1993 Revision and Commetary Criminal Intelligence Systems Operating Policies

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule

SUMMARY: The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines.

EFFECTIVE DATE: September 16, 1993

FOR FURTHER INFORMATION CONTACT: Paul Kendall, Esquire, General Counsel, Office of Justice Programs, 633 Indiana Ave., NW, Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235.

SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691).

The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows:

CONFIDENTIALITY OF INFORMATION

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the

funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed \$10,000, in addition to any other penalty imposed by law.

28 CFR Part 23: 1998 Policy Clarification Criminal Intelligence Systems Operating Policies

[Federal Register: December 30, 1998 (Volume 63, Number 250)]

[Page 71752-71753]

From the Federal Register Online via GPO Access [wais.access.gpo.gov]

DEPARTMENT OF JUSTICE

28 CFR Part 23

[OJP(BJA)-1177B]

RIN 1121-ZB40

CRIMINAL INTELLIGENCE SHARING SYSTEMS; POLICY CLARIFICATION

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street N.W, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

COMMENTS

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is “information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and *** [m]eets criminal intelligence system submission criteria.” Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if “there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.” 28 CFR 23.20(b) extends that limitation to collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 C.F.R. Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this

section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing “Comment” or “Modus Operandi” fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional “Northwest Market.” An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of “Northwest Market” would not be permitted, because there was no

reasonable suspicion that the “Northwest Market” was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the “Northwest Market” was clearly noted to be non-criminal in nature. For example, the data field in which “Northwest Market” was entered could be marked “Non-Criminal Identifying Information,” or the words “Northwest Market” could be followed by a parenthetical comment such as “This organization has been entered into the system for identification purposes only-it is not suspected of any criminal activity or involvement.” A criminal intelligence system record or file could not be created for “Northwest Market” solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on “Northwest Market.” Further, the fact that other individuals frequent “Northwest Market” would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

THE DEFINITION OF A “CRIMINAL INTELLIGENCE SYSTEM”

The definition of a “criminal intelligence system” is given in 28 CFR 23.3(b)(1) as the “arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information ***.” Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

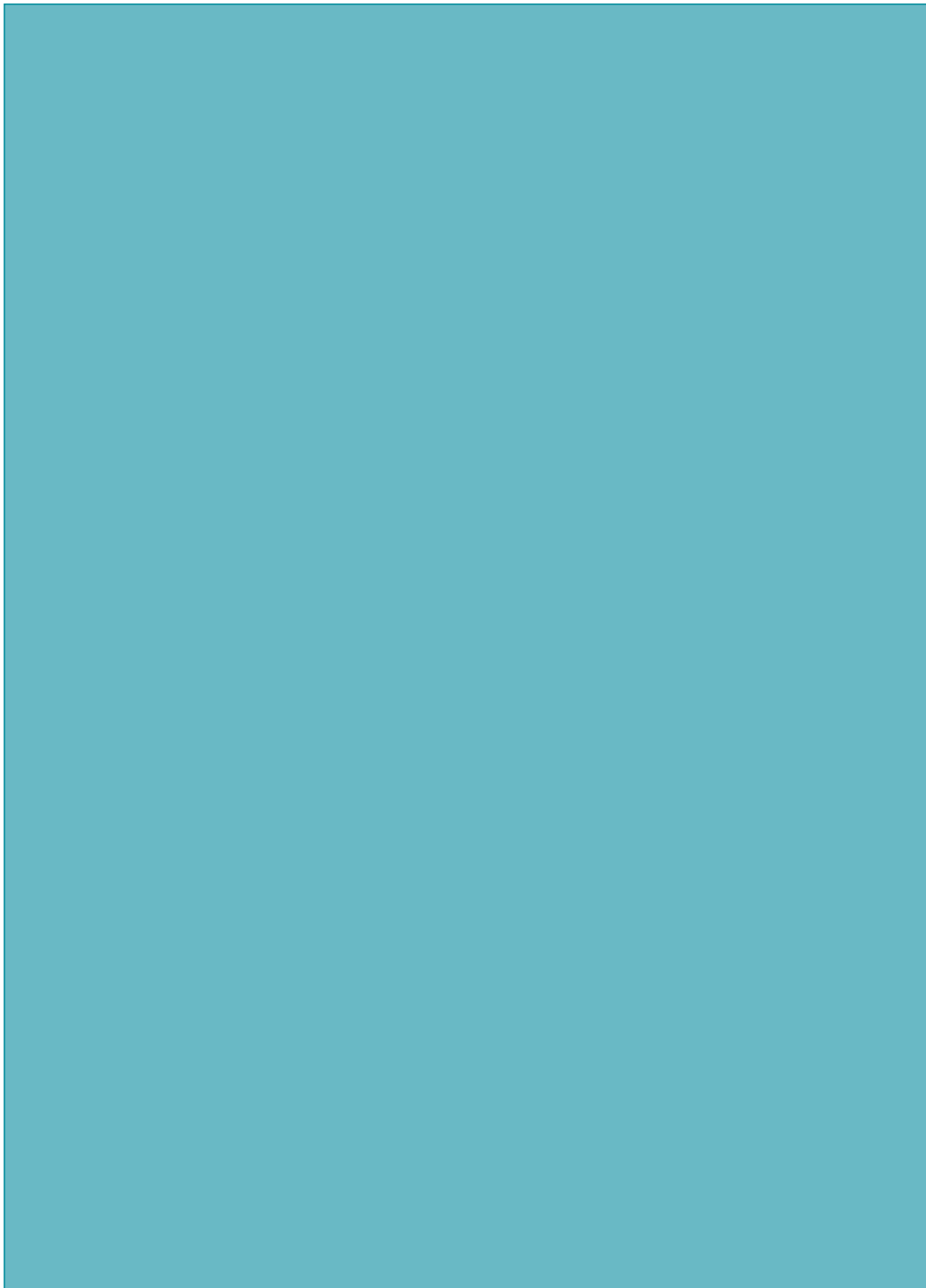
The comments to the 1993 revision of 28 CFR Part 23 noted that “[t]he term ‘intelligence system’ is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation ***.” 58 FR 48448-48449 (Sept. 16,

1993.) The comments further noted that materials that “may assist an agency to produce investigative or other information for an intelligence system ***” do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of “criminal intelligence system,” suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

APPENDIX E



FBI Security Clearance

Federal Security Clearance Process for the FBI

It is the policy of the Federal Bureau of Investigation (FBI) to share with Law Enforcement personnel pertinent information regarding terrorism. In the past, the primary mechanism for such information sharing was the Joint Terrorism Task Force (JTTF). In response to the terrorist attack on America on September 11, 2001, the FBI established the State and Local Law Enforcement Executives and Elected Officials Security Clearance Initiative. This program was initiated to brief officials with an established “need-to-know” on classified information that would or could affect their area of jurisdiction.

Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. This brochure describes when security clearances are necessary and the notable differences between clearance levels. It also describes the process involved in applying and being considered for a clearance. State and local officials who require access to classified material must apply for a security clearance through their local FBI Field Office. The candidate should obtain from their local FBI Field Office a Standard Form 86 (SF 86), Questionnaire for National Security Positions; and two FD-258 (FBI applicant fingerprint cards). One of two levels of security clearance, Secret or Top Secret, may be appropriate.

The background investigation and records checks for Secret and Top Secret security clearance are mandated by Presidential Executive Order (EO). The EO requires these procedures in order for a security clearance to be granted; the FBI does not have the ability to waive them.

Secret Clearances

A Secret security clearance may be granted to those persons that have a “need-to-know” national security information, classified at the Confidential or Secret level. It is generally the most appropriate security clearance for state and local law enforcement officials that do not routinely work on an

FBI Task Force or in an FBI facility. A Secret security clearance takes the least amount of time to process and allows for escorted access to FBI facilities.

The procedure is as follows:

FBI performs record checks with various Federal agencies and local law enforcement, as well as, a review of credit history.

Candidate completes forms SF-86 and FD-258. Once favorably adjudicated for a Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

Top Secret Clearances

A Top Secret clearance may be granted to those persons who have a “need-to-know” national security information, classified up to the Top Secret level, and who need unescorted access to FBI facilities, when necessary. This type of clearance will most often be appropriate for law enforcement officers assigned to FBI Task Forces housed in FBI facilities. In addition to all the requirements at the Secret level, a background investigation, covering a 10-year time period, is required. Once favorably adjudicated for a Top Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

Questions and Answers (Q&A)

Q: Who should apply for a security clearance?

A: State or local officials whose duties require that they have access to classified information, and who are willing to undergo a mandatory background investigation.

Q: What is the purpose of a background investigation?

A: The scope of the investigation varies with the level of the clearance being sought. It is designed to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information. Applicants must meet certain criteria, relating to

their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals.

Q: If an individual occupies an executive position with a law enforcement agency, must he or she still undergo a background investigation in order to access classified information?

A: An Executive Order (EO), issued by the President, requires background investigations for all persons entrusted with access to classified information. The provisions of the EO are mandatory, cannot be waived, and apply equally to all federal, state, and local law enforcement officers. This is true of both Secret and Top Secret security clearances.

Q: How long does it normally take to obtain a Secret security clearance?

A: It is the goal of the FBI to complete the processing for Secret security clearances within 45 to 60 days, once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity.

Q: How long does it normally take to obtain a Top Secret security clearance?

A: It is the goal of the FBI to complete the processing for Top Secret security clearances within 6 to 9 months, once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity.

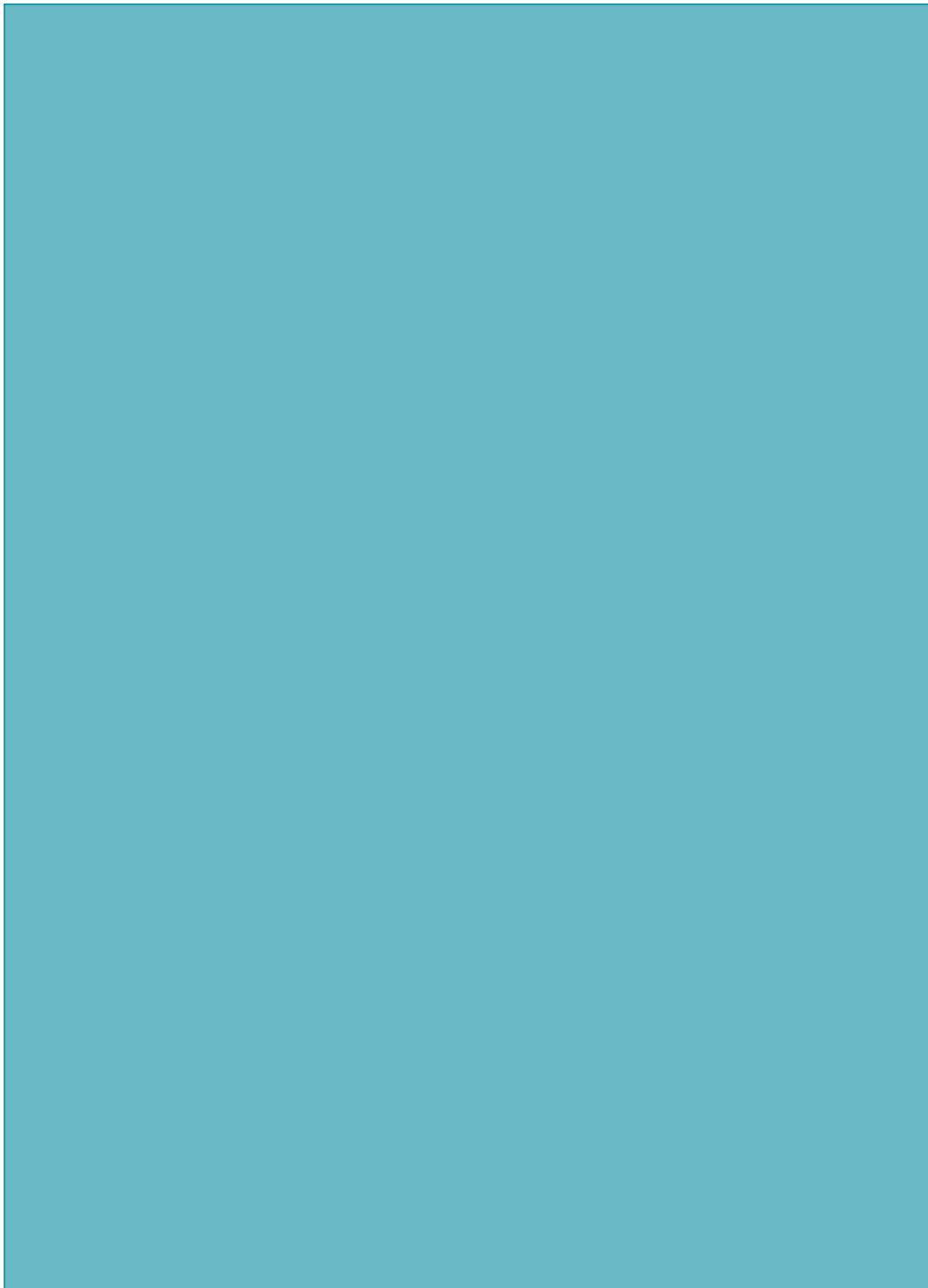
Q: What kind of inquiries will the FBI make into my background?

A: Credit and criminal history checks will be conducted on all applicants. For a Top Secret security clearance, the background investigation includes additional record checks which can verify citizenship for the applicant and family members, verification of birth, education, employment history, and military history. Additionally, interviews will be conducted of persons who know the candidate, and of any spouse divorced within the past ten years. Additional interviews will be conducted, as needed, to resolve any inconsistencies. Residences will be confirmed, neighbors interviewed, and public records queried for information about bankruptcies, divorces, and criminal or civil litigation. The background investigation may be expanded if an applicant has resided abroad, or has a history of mental disorders, or drug or alcohol abuse. A personal interview will be conducted of the candidate.

- Q:** If I have a poor credit history, or other issues in my background, will this prevent me from getting a security clearance?
- A:** A poor credit history, or other issues, will not necessarily disqualify a candidate from receiving a clearance, but resolution of the issues will likely take additional time. If the issues are significant, they may prevent a clearance from being approved.
- Q:** If I choose not to apply for a security clearance, will I still be informed about counterterrorism issues important to my jurisdiction?
- A:** Absolutely. If the FBI receives information relevant to terrorism which may impact your jurisdiction, you will be informed by your local Field Office, through the Law Enforcement On- Line network, via NLETS, and through other available mechanisms which are approved for the transmission of unclassified information. Most terrorism-related information can be provided in an unclassified form.
- Q:** Are there any other advantages or disadvantages to receiving unclassified or classified terrorism related information?
- A:** An additional advantage of receiving unclassified terrorism-related information is that there may be fewer restrictions on your ability to further disseminate it within your jurisdiction. Classified information may only be disseminated to other cleared persons, who also have a need-to-know.
- Q:** What is the difference between an interim and a full security clearance?
- A:** Interim clearances are granted in exceptional circumstances where official functions must be performed before completion of the investigative and adjudicative processes associated with the security clearance procedure. There is no difference between an interim and a full security clearance as it relates to access to classified information. However, when such access is granted, the background investigation must be expedited, and, if unfavorable information is developed at anytime, the interim security clearance may be withdrawn.

If you have any additional questions, and/or wish to apply for a security clearance, please contact your local FBI field office. (See <http://www.fbi.gov/contact/fo/fo.htm> to locate the nearest field office.)

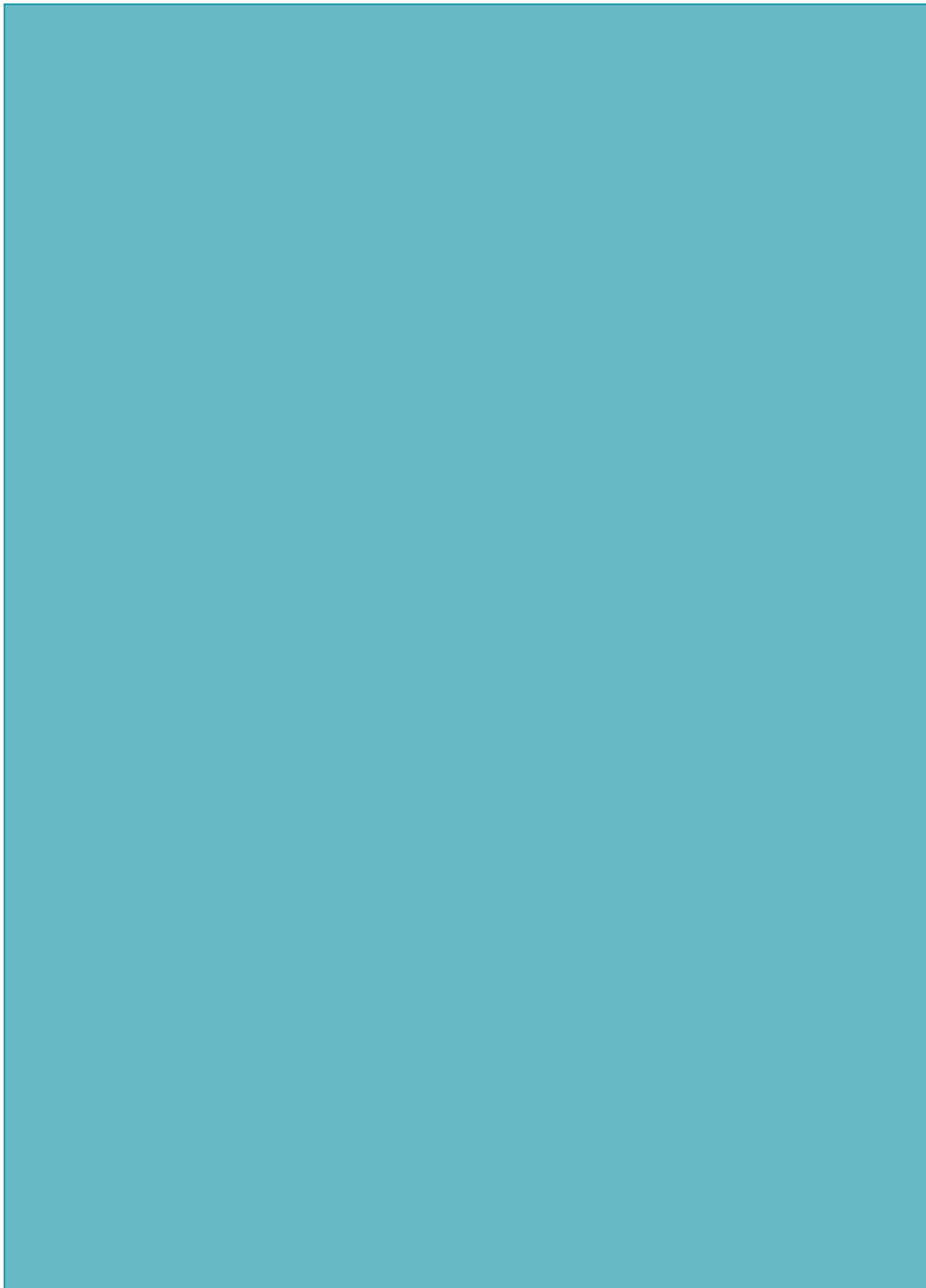
APPENDIX F



Biography of David L. Carter, Ph.D.

David L. Carter (Ph.D., Sam Houston State University) is a professor in the School of Criminal Justice and director of the Intelligence Program at Michigan State University. A former Kansas City, Missouri police officer, Dr. Carter was chairman of the Department of Criminal Justice at the University of Texas-Pan American in Edinburg, Texas for 9 years prior to his appointment at Michigan State in 1985. He has served as a trainer, consultant, and advisor to many law enforcement agencies throughout the U.S., Europe, and Asia on matters associated with officer behavior, community policing, law enforcement intelligence, and computer crime. In addition, he has presented training sessions at the FBI National Academy, the FBI Law Enforcement Executive Development Seminar (LEEDS); the International Law Enforcement Academy in Budapest, Hungary; the United Nations Asia and Far East Institute (UNAFEI) in Tokyo; police “command colleges” of Texas, Florida, Ohio, Massachusetts, Wisconsin, and Kentucky; and served at the FBI Academy's Behavioral Science Services Unit the first academic faculty exchange with the Bureau. Dr. Carter is also an instructor in the Bureau of Justice Assistance SLATT program, author of the COPS-funded publication, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*, and project director of the managerial intelligence training program funded by the Department of Homeland Security. He is a fellowship recipient from the Foundation for Defending Democracies where he studied terrorism in Israel. In addition to teaching graduate and undergraduate courses at Michigan State, Dr. Carter is director of the Criminal Justice Overseas Study Program to England. He is the author or co-author of five books and numerous articles and monographs on policing issues and is a member of the editorial boards of various professional publications. His most recent book is the seventh edition of the widely-used community relations textbook, *The Police and Community*, (published by Prentice-Hall). He has another book forthcoming from Prentice-Hall entitled *Homeland Security for State and Local Police*.

APPENDIX G



Intelligence Unit Management Audit (Tear-Out Section)

Audit Factors for the Law Enforcement Intelligence Function

Section A. Meeting National Standards

1. Does the police department subscribe to the tenets and standards of the *Global Justice Information Sharing Initiative*?
☐ Yes ☐ No
2. Does the police department subscribe to the standards of the *National Criminal Intelligence Sharing Plan*?
☐ Yes ☐ No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the Office of Domestic Preparedness *Guidelines for Homeland Security*?
☐ Yes ☐ No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 *Criminal Intelligence*?
☐ Yes ☐ No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) *Model Criminal Intelligence Policy*?
☐ Yes ☐ No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines*?
☐ Yes ☐ No
7. Does the police department subscribe to the IACP *Code of Ethics* or have an articulated Code of Ethics?
☐ Yes ☐ No
8. Does the police department subscribe to the IACP *Code of Conduct* or have an articulated Code of Conduct?
☐ Yes ☐ No
9. Does the police department have an articulated Statement of Values?
☐ Yes ☐ No

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



10. Does the police department adhere to the regulations of 28 CFR Part 23 for its Criminal Intelligence Records System?
☐ Yes ☐ No
 - a. Does the police department operate a federally funded multi-jurisdictional criminal intelligence records system?
☐ Yes ☐ No
11. Does the police department subscribe to the tenets of the *Justice Information Privacy Guidelines*?
☐ Yes ☐ No
12. Does the police department subscribe to the tenets for information system security defined in the report, *Applying Security Practices to Justice Information Sharing*?
☐ Yes ☐ No
13. Does the law enforcement agency subscribe to the philosophy of *Intelligence-Led Policing*?
☐ Yes ☐ No
14. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious or doctrinal purpose?
☐ Yes ☐ No

Section B: Management Issues

1. Has a mission statement been written for the Intelligence Unit?
☐ Yes ☐ No
2. Is the purpose and role of the Unit clearly articulated and related to the Police Department's Mission Statement?
☐ Yes ☐ No
3. Have priorities been established for the types of crimes the Unit will address?
☐ Yes ☐ No
 - a. Is any written rationale provided for these priorities?
☐ Yes ☐ No
4. Are expected activities of the unit articulated?
☐ Yes ☐ No
5. Does the mission statement express ethical standards?
☐ Yes ☐ No

6. Does the mission statement express the importance of protecting citizens' rights?

☐ Yes ☐ No

1. Policies and Procedures

1. Are there written and officially articulated policies and procedures for management of the intelligence function?

☐ Yes ☐ No

2. Have intelligence policies been formed to minimize the discretion of information collectors?

☐ Yes ☐ No

If Yes, Describe:

3. Is there a policy and procedures on "Information Collection"?

☐ Yes ☐ No

If Yes, Describe:

Law Enforcement

Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.

School of Criminal Justice
Michigan State University



2. Management of Information: Definitional Standards

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?

☐ Yes ☐ No

2. What is the source of the definitions?

☐ NCISP ☐ Federal Agency

☐ Mixed ☐ N/A

**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



3. Has the department articulated standards for classifying information in the Intelligence Unit?

☐ Yes ☐ No

Priority	Classification	Description	Release Authority
Highest Level	Sensitive	Current corruption case; complex criminality; confidential informants	Dept Executive or Intelligence Cmdr.
Medium Level	Confidential	Non-sensitive information through intelligence channels; Law Enforcement only	Intelligence Unit Cmdr or Supervisor
Lowest Level	Restricted	LE use but no need for high security	Intell Unit Personnel
Unclassified	Public Access	Information that may be released to public and media	Intell Unit Personnel

4. How are those standards monitored and enforced?

☐ Supervisor ☐ Other

5. Does the department have a system for assessing the reliability of sources that provide information that will be retained in the Intelligence Records System?

☐ Yes ☐ No

6. Are there standardized definitions of the reliability scale?

☐ Yes ☐ No

7. Does the department have a system for assessing the validity of the information that will be retained in the Intelligence Records System?

☐ Yes ☐ No

8. Are there standardized definitions of the validity scale?

☐ Yes ☐ No

9. Does the Intelligence Unit have operational definitions that can be applied to a person under investigation or a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a "permanent file" or a "temporary file"?

☐ Yes ☐ No

If Yes...

- a. Are the types of identifying information that should be placed in the file articulated?

☐ Yes ☐ No

- b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?

☐ Yes ☐ No

- c. Is there a procedure articulating the conditions wherein a temporary file may be created?
☐ Yes ☐ No
- d. Does the procedure specify a time limit that the temporary file can be kept?
☐ Yes ☐ No
- e. Is there an operational definition of "Non-Criminal Identifying Information" and procedures for recording and retaining this information?
☐ Yes ☐ No
- f. Are there clear procedures that *describe* the types of information that should not be entered into the Intelligence Records System?
☐ Yes ☐ No

3. Management of Information: Source Documents

- 1. Does the department have a written directive explaining the different types of source documents that will be entered in the Intelligence Records System?
☐ Yes ☐ No
- 2. What types of source documents are entered into the Intelligence Records System?
Describe:
- 3. Does the police department have a written directive that the rationale for each source document entered into the Intelligence Records System must be articulated in a report or notation?
☐ Yes ☐ No

Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



4. Management of Information: Data Entry

1. Who is responsible for entering information into the Intelligence Records System?
Position/Classification:

2. Who supervises the information entry process?
Position/Classification:

5. Management of Information: Accountability

1. Who is the Custodian of the Intelligence Records System that ensures all regulations, law, policy and procedures are being followed?
Position/Classification:

2. Is there a person external to the Intelligence Unit who is designated to monitor the Intelligence Records System and related processes?
☐ Yes ☐ No
If Yes, Position/Classification):

3. Does the department have written procedures for the retention of records in the Intelligence Records System?
☐ Yes ☐ No

6. Management of Information: Retention and Purging of Records

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?
☐ Yes ☐ No
2. Does the retention policy and procedure include written criteria for purging information?
☐ Yes ☐ No

3. How often does a review and purge process occur?

Frequency:

4. What is the purge process?

Describe:

5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy and relevancy?

☐ Yes ☐ No

6. Does the purge process require destruction of the source document and removal of all references to the document to be purged if the information is no longer appropriate for retention?

☐ Yes ☐ No

7. What is the destruction process for purged "hard copy" records?

Describe:

8. After information has been purged from a computerized Intelligence Records System, is free space on the hard drive and/or specific purged files electronically "wiped"?

☐ Yes ☐ No

- a. Are back-ups wiped?

☐ Yes ☐ No

Law Enforcement

Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



- b. What is the accountability system for purging back-ups?
Describe:

9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?

☐ Yes ☐ No

10. What is the process for purging partial information from “hard copy” source documents?

Describe:

11. Who is responsible for ensuring compliance of the purge process?
Position/Classification:

7. Management of Information: Personal/Individually-Held Records and Files

1. Is there an intelligence unit policy and procedures concerning the retention of individual notes and records that identifies persons wherein criminality is suspected but is not in either a temporary or permanent file and is not entered into any formal records system or database?

☐ Yes ☐ No

a. How is the possession of personal records monitored?

☐ Yes ☐ No

b. How is the policy enforced?

☐ Yes ☐ No

8. Management of Information: Accessing Intelligence Records

1. Is access to the Intelligence Records limited?

☐ Yes ☐ No

2. If yes, who may access the Intelligence Records System?

Describe:

3. What security controls exist for accessing computerized records?

Describe:

4. Can the computerized records system be accessed through remote access?

☐ Yes ☐ No

a. If so, what security controls exist for remote access?

Describe:

Law Enforcement

Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



5. How are physical records stored?
Describe:
6. Who grants access privileges to Intelligence Records?
Position/Classification:
7. Who has access to records?
Position/Classification:
8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?
☐ Yes ☐ No
9. What audit process is in place for access to computerized records?
Describe:
10. What audit process is in place for access to physical records?
Describe:

11. How are physical records secured?

Describe:

12. What process is in place to handle unauthorized access to intelligence physical records?

Describe:

13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?

Describe:

Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University

9. Physical Location of the Intelligence Unit and Records

1. Sufficiency: Is the Intelligence Unit in a physical location that has sufficient space to perform all of its responsibilities?

☐ Yes ☐ No

2. Security: Is the Intelligence Unit in a physical location wherein the entire workspace may be completely secured?

☐ Yes ☐ No

a. Is there adequate secured storage cabinets (or a vault) for (1) documents classified by the Intelligence Unit and (2) sensitive records storage within the intelligence unit's physical location?

☐ Yes ☐ No



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



- b. Is there adequate security and segregated storage for federally classified documents within the intelligence unit?
☐ Yes ☐ No
- 1) Is that storage accessible only by persons with a federal top secret security clearance?
☐ Yes ☐ No
- 3. Convenience: Is the Intelligence Unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?
☐ Yes ☐ No

10. Tangential Policy Issues: Criminal Informants and Undercover Operations

- 1. Is there a formally articulated policy and procedures for managing criminal informants?
☐ Yes ☐ No
 - a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?
☐ Yes ☐ No
 - b. Are informant files secured separately from intelligence files?
☐ Yes ☐ No
- 2. Is there a formally articulated policy and procedures concerning undercover operations that apply to members of the Intelligence Unit?
☐ Yes ☐ No
- 3. Does the police department have a policy on alcohol consumption for officers working undercover?
☐ Yes ☐ No
 - a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?
☐ Yes ☐ No
- 4. Does the police department have a "narcotics simulation" policy and training for undercover officers?
☐ Yes ☐ No
- 5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?
☐ Yes ☐ No

6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?
☐ Yes ☐ No
7. With respect to undercover operating funds:
- a. Is there a 1-tier or 2-tier process to approve use of the funds?
☐ 1 Tier ☐ 2 Tier
- b. Is a written report required to document expenditure of the funds?
☐ Yes ☐ No
- c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?
Days ☐ No Set Time
- d. Is there a regular external audit of undercover funds?
☐ Yes [How Often?] ☐ No

Section C: Personnel

1. Is a position classification plan in place that provides a clear job description for each position in the unit?
☐ Yes ☐ No
2. Is a position classification plan in place that articulates Knowledge, Skills and Abilities (KSAs) for each position?
☐ Yes ☐ No
3. Is there sufficient hierarchical staff (managers/supervisors) assigned to the unit to effectively perform supervisory responsibilities?
☐ Yes ☐ No
4. Is there sufficient functional staff (analysts and/or investigators) to effectively fulfill defined unit responsibilities?
☐ Yes ☐ No
5. Is there sufficient support staff (secretaries, clerks) to effectively support the unit's activities?
☐ Yes ☐ No
6. Does the screening process for nonsworn employees of the intelligence unit require:
- a. Fingerprint check?
☐ Yes ☐ No
- b. Background investigation
☐ Yes ☐ No

Law Enforcement

Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



7. If the Intelligence Unit has non-PD employees assigned to it – e.g., National Guard analysts, personnel from the state or local law enforcement agencies – would there be a screening process for those persons?

☐ Yes ☐ No

If Yes, Describe:

1. Training

1. What types of training do preservice and newly assigned personnel receive?

☐ None ☐ Some–Describe:

- a. Are newly assigned sworn employees to the Intelligence Unit required to attend 28 CFR Part 23 training?

☐ Yes ☐ No

- b. Are newly hired or assigned non-sworn employees required to attend 28 CFR Part 23 training?

☐ Yes ☐ No

2. What types of training do in-service personnel receive?

☐ None ☐ Some

Describe:

3. Have members of the Intelligence Unit attended any of the following federal government intelligence training programs which are open to state and local law enforcement officers?
- a. DEA Federal Law Enforcement Analyst Training (FLEAT)?
☐ Yes ☐ No
 - b. FBI College of Analytic Studies?
☐ Yes ☐ No
 - c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course?
☐ Yes ☐ No
 - d. National Drug Intelligence Center Basic Intelligence Analysis Course?
☐ Yes ☐ No
 - e. National White Collar Crime Center Foundations of Intelligence Analysis?
☐ Yes ☐ No
 - f. Regional Counterdrug Training Academy Intelligence Operations Course?
☐ Yes ☐ No

2. Supervision

- 1. Does supervision effectively monitor adherence to written procedures?
☐ Yes ☐ No
- 2. Does supervision effectively monitor adherence to guidelines adopted by the department?
☐ Yes ☐ No
- 3. Are performance evaluations tied directly to the job descriptions?
☐ Yes ☐ No
- 4. Does supervision effectively monitor the performance of required duties (Including the quality of performance)?
☐ Yes ☐ No
- 5. Is supervision effectively monitoring personnel to ensure civil rights allegations cannot be made with respect to negligent:
 - a. Failure to train?
☐ Yes ☐ No

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



- b. Hiring?
☐ Yes ☐ No
 - c. Failure to supervise?
☐ Yes ☐ No
 - d. Assignment?
☐ Yes ☐ No
 - e. Failure to direct?
☐ Yes ☐ No
 - f. Failure to discipline?
☐ Yes ☐ No
 - g. Entrustment?
☐ Yes ☐ No
6. Is there effective supervision of the Intelligence Unit throughout the chain of command external to the Intelligence Unit?
☐ Yes ☐ No

Section D: Fiscal Management

- 1. Is the budget sufficient to fulfill the stated mission?
☐ Yes ☐ No
- 2. Does the Intelligence Commander have input into the budget planning process?
☐ Yes ☐ No
- 3. Is there over-reliance on “soft money” to operate the unit?
☐ Yes ☐ No
- 4. Are equipment and personnel line items assigned directly to the Intelligence Unit?²³⁵
☐ Yes ☐ No
- 5. Is there an established process for reliably monitoring credit cards assigned to personnel?
☐ Yes ☐ No ☐ NA

Section E: Unit Evaluation

- 1. As a whole, is the unit effective with respect to:
 - a. Providing information to prevent crime?
☐ Yes ☐ No

- b. Providing information to apprehend criminals?
☐ Yes ☐ No
- c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?
☐ Yes ☐ No
2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence unit's productivity as an organizational entity?
- a. Number and type of analytic products delivered for investigative purposes?
☐ Yes ☐ No ☐ NA
- b. Number and type of analytic products that led to arrest?
☐ Yes ☐ No ☐ NA
- c. Assets seized from illegal activities wherein intelligence contributed to the arrest and/or seizure?
☐ Yes ☐ No ☐ NA
- d. Number and types of strategic intelligence products delivered to the command staff?
☐ Yes ☐ No ☐ NA
- e. Number of intelligence-sharing meetings attended by unit staff?
☐ Yes ☐ No ☐ NA
- f. Number of briefings provided by the intelligence staff?
☐ Yes ☐ No ☐ NA
- g. Total number of queries into the intelligence data base?
☐ Yes ☐ No ☐ NA
- h. Number of permanent files opened?
☐ Yes ☐ No ☐ NA
- i. Number of temporary files investigated?
☐ Yes ☐ No ☐ NA
- j. Number of requests for information to the unit from outside agencies?
☐ Yes ☐ No ☐ NA
3. Are products produced by the Intelligence Unit:
- a. In a consistent format?
☐ Yes ☐ No
- b. Easily consumed and used (i.e., understandable and actionable)?
☐ Yes ☐ No

Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



**Law Enforcement
Intelligence:**
A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



- c. Contain timely information and disseminated in a timely manner?
☐ Yes ☐ No
- d. Have substantive contact to aid in preventing or controlling crime?
☐ Yes ☐ No
- 4. Given the confidential nature of the information contained in the Intelligence Unit, is there a policy and procedures if a city, county, state, or federal fiscal or program auditor seeks to audit the Intelligence Unit?
☐ Yes ☐ No
If Yes, Describe:

Section F. Collection

- 1. Is there an articulated collection plan for the Intelligence Unit?
☐ Yes ☐ No
If Yes, Describe:
 - a. How often and when is the plan updated?
Describe:
- 2. Have the following activities been performed by the Intelligence Unit:
 - a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists?
☐ Yes ☐ No
 - b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region?
☐ Yes ☐ No
 - c. A target or criminal commodity analysis of the region?
☐ Yes ☐ No
 - d. A target or criminal commodity vulnerability assessment in the region?
☐ Yes ☐ No
- 3. For each identified threat, have intelligence requirements been articulated?
☐ Yes ☐ No

- a. If Yes, Describe the methods of collection that will be used to fulfill those intelligence requirements.

Section G: Technology and Networking

1. Are any members of the Intelligence Unit subscribed members to the FBI's secure Email system Law Enforcement Online (LEO)?
☐ Yes--All ☐ Yes--Some ☐ No
2. Are any members of the Intelligence Unit subscribed members to the secure Regional Information Sharing System (RISS) email system riss.net?
☐ Yes--All ☐ Yes--Some ☐ No
 - a. If yes, are the RISS databases (e.g., RISS.gang, ATIX, etc.) regularly used?
☐ Yes ☐ No
3. Is the police department a member of the Regional Information Sharing System?
☐ Yes ☐ No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted via the National Law Enforcement Teletype System (NLETS) are forwarded to the Intelligence Unit?
☐ Yes ☐ No
5. Are you connected to any state-operated intelligence or information networks?
☐ Yes ☐ No
If Yes, Describe:

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



Law Enforcement Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University



6. Are you connected to any regional intelligence or information networks (including HIDTA)?

☐ Yes ☐ No

If Yes, Describe:

7. Does the intelligence have access and use the National Virtual Pointer System (NVPS)?

☐ Yes ☐ No

8. Is there a formal approval process for entering into a memorandum of understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?

☐ Yes ☐ No

If Yes, Describe the process:

Who must approve the MOU?

Section H: Legal Issues

1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?
- ☐ Yes ☐ No
2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the intelligence unit?
- ☐ Yes ☐ No

3. Is there a designated person the police department contacts in response to a subpoena for a file in the Intelligence Records System?
☐ Yes ☐ No
4. Does the Intelligence Unit Commander have a legal resource for advice to help protect intelligence records from objectionable access?
☐ Yes ☐ No
5. Does the Intelligence Unit Commander have a legal resource for advice on matters related to criminal procedure and civil rights?
☐ Yes ☐ No
6. Does the Intelligence Unit Commander have a legal resource for advice on matters related to questions of civil liability as it relates to all aspects of the intelligence function?
☐ Yes ☐ No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
☐ Yes ☐ No

Law Enforcement

Intelligence:

A Guide for State, Local,
and Tribal Law
Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University





Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies

To obtain details on COPS programs, call the
COPS Office Response Center at 800.421.6770

Visit COPS Online at www.cops.usdoj.gov

e09042536 October 28, 2004
ISBN: 1-932582-44-4